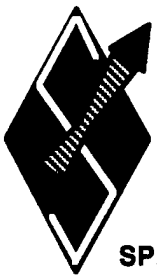
CDRL #004



SPARTA, INC.

# DoD Supplements Recommendations for GOSIP

February 28, 1990

Contract No. DCA100-89-C-0001

Prepared for:

Defense Communications Engineering Center
Defense Communications Agency
Code R640, ATTN: COR
1860 Wiehle Avenue
Reston, VA 22090-5500





SPARTA, Inc.
7926 Jones Branch Drive
Suite 1070
McLean, VA 22102
(703) 448-0210

SECURITY CLASSIFICATION OF THIS PAGE

# REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188
Exp Date: Jun 30, 1986

| | |
|---|---|
| 1a. REPORT SECURITY CLASSIFICATION<br>Unclassified | 1b. RESTRICTIVE MARKINGS<br>None |
| 2a. SECURITY CLASSIFICATION AUTHORITY | 3. DISTRIBUTION/AVAILABILITY OF REPORT<br>Unlimited |
| 2b. DECLASSIFICATION/DOWNGRADING SCHEDULE | |
| 4. PERFORMING ORGANIZATION REPORT NUMBER(S) | 5. MONITORING ORGANIZATION REPORT NUMBER(S) |
| 6a. NAME OF PERFORMING ORGANIZATION<br>SPARTA, INC. — 6b. OFFICE SYMBOL (If applicable) | 7a. NAME OF MONITORING ORGANIZATION<br>Defense Communication Engineering Center |
| 6c. ADDRESS (City, State, and ZIP Code)<br>7926 Jones Branch Drive, Suite 1070<br>McLean, VA 22102 | 7b. ADDRESS (City, State, and ZIP Code)<br>1860 Wiehle Avenue<br>Reston, VA 22091 |
| 8a. NAME OF FUNDING/SPONSORING ORGANIZATION<br>Defense Communications Agency — 8b. OFFICE SYMBOL (If applicable)<br>R640 | 9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER<br>DCA100-89-C-0001 |
| 8c. ADDRESS (City, State, and ZIP Code)<br>Washington, D. C. | 10. SOURCE OF FUNDING NUMBERS<br>PROGRAM ELEMENT NO. — PROJECT NO. — TASK NO — WORK UNIT ACCESSION NO. |

11. TITLE (Include Security Classification)
DOD Supplements Recommendations for GOSIP

12. PERSONAL AUTHOR(S)
R.T. Harris, C.A. Eldridge, J.E. Swanson

| 13a. TYPE OF REPORT | 13b. TIME COVERED | 14. DATE OF REPORT (Year, Month, Day) | 15. PAGE COUNT |
|---|---|---|---|
| Final | FROM 8/29/89 TO 2/28/90 | 1990 February 28 | |

16. SUPPLEMENTARY NOTATION

| 17 COSATI CODES | | | 18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number) |
|---|---|---|---|
| FIELD | GROUP | SUB-GROUP | GOSIP |
| | | | |
| | | | |

19. ABSTRACT (Continue on reverse if necessary and identify by block

This technical report recommends steps needed to adapt Government Open System Interconnection Profile (GOSIP) Communication protocols for DoD use. The report provides a set of recommendations consistent with the GOSIP specification for communication protocols allowing primary, secondary and tertiary sources of information to be used for procurement of communication protocols. These recommendations are grouped into three areas: specifying options available in the primary sources but not selected by GOSIP, augmenting existing protocols with tertiary specifications and identification of research areas where solutions do not exist today.

| 20. DISTRIBUTION/AVAILABILITY OF ABSTRACT | 21. ABSTRACT SECURITY CLASSIFICATION |
|---|---|
| ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS | Unclassified |
| 22a. NAME OF RESPONSIBLE INDIVIDUAL<br>Mr. James Tontonoz | 22b. TELEPHONE (Include Area Code)<br>(703) 437-2038 — 22c. OFFICE SYMBOL<br>R640 |

DD FORM 1473, 84 MAR — 83 APR edition may be used until exhausted. All other editions are obsolete.

SECURITY CLASSIFICATION OF THIS PAGE

## Executive Summary

The purpose of this technical report is to recommend those steps needed to adopt Government Open System Interconnection Profile (GOSIP) communication protocols for DoD use. These recommendations will assure the DoD technical communication needs are met after a transition to GOSIP. This technical report does not identify any technical concerns serious enough to advise a halt to the transition to the Open Systems Interconnection Protocols (OSI) as defined in GOSIP. The report provides a set of recommendations consistent with the GOSIP specification for communication protocols allowing primary, secondary and tertiary sources of information to be used for procurement of communication protocols. These recommendations are grouped into three areas; specifying options available in the primary sources but not selected by GOSIP, augmenting existing protocols with tertiary specifications and identification of research areas where solutions do not exist today.

The technical recommendations that can be obtained by specifying the options available within the primary sources such as International Standards Organization (ISO) specifications are the following:

- Session Protocol Version 2,
- Message Handling System (MHS) smart splitting/duplication option,
- making use of the Quality of Service Parameters and adopting the National Institute of Science and Technology (NIST) Priority Proposal, and
- making use of the Transport Protocol options.

The Session Protocol Version 2 allows unlimited data size negotiation, as opposed to limiting data size to 512 octets which can enhance the efficiency of communications channels. The MHS smart splitting/duplication option provides some limited multicast capability which can enhance the efficiency of mass message transmissions. Finally, the QoS parameters for priority, delay, throughput, security, error rate should be used to encourage vendors to implement mechanisms that could enhance system operation. The semantics of the priority parameter can be standardized by accepting the NIST Implementor Agreements proposal on consistent levels of priority within the end systems. These improvements can be obtained by specifying existing options to the ISO specifications by acquisition authorities in future procurements.

The next area of technical recommendations consist of modifications of existing protocols. The recommendations include the following:

- implementation of the advanced technology for congestion avoidance,
- best effort multicast and other extensions to the transport layer protocol,
- developing a security profile to specify the use of Secure Data Networking System (SDNS) mechanisms,
- using a "thin" protocol stack and
- extending the 16 bit checksum to 32 bits in the link layer protocol.

The extensions to the transport protocol make use of advanced technology developed within the DoD Internet and integrate it with the GOSIP transport layer protocol to give more efficient operation. The development of a security profile is necessary to assist acquisition authorities the proper placement of SDNS mechanisms and specifying an adequate access control policy. The thin protocol stacks are a minimum subset of the GOSIP protocol stack to provide access to dumb network components (modems) and to provide better service for tactical and real time users to reduce system overhead. The 32 bit checksum extension should provide better data integrity at a minimal increase in the parameter field width and is already in use in some of the link layer protocols. These changes require some modification of the existing protocol standards and evaluation before changing the standards.

The final area of technical recommendations are the identification of research areas that need to be developed further before recommending a specific solution to the DoD communication needs. These areas include the research and development of a QoS framework so that network users can specify and receive (and be charged) specific communications channel characteristics that are necessary for there missions. Another area requiring further research is the development of a reliable multicast protocol that can provide service to a dynamic group.

This report has adopted the NATO Military Features and PSTP Military Issues as valid military needs. We have analyzed the high level requirements for these military topics in a previous technical report[1] and use them as guidance when recommending a solution among alternatives

[1]Analysis and Determination of U.S. DoD Requirements and Services for ISO Protocols, dated August 28, 1989, SPARTA, Inc.

to the military communication services. The NATO Military Features and PSTP Military Issues are defined , solutions evaluated and recommendations given in section two. The recommendations are grouped into the appropriate GOSIP protocol layer in section three to form a complete DoD supplemental protocol stack. The following paragraphs provide a brief overview of the report.

Solutions to the military needs defined by the NATO Military Features and the PSTP Military Issues are presented in section three. For each of the military needs, a definition of the associated technical problems, background discussion on potential approaches for resolving the issues and recommendations for near-term solutions are presented. A brief summary for each issue is presented in the following paragraphs:

The Multi-Homed and Mobile End System issue can be addressed using dynamic routing. These capabilities are inherent to the International Standards Organization (ISO) routing protocols End System to Intermediate System (ES-IS) and Intermediate System to Intermediate System (IS-IS) protocols.

The Multi-Peer Data Transmission (MPDT) issue can be addressed by developing two new military standards; a best delivery effort protocol at the network layer, and a reliable delivery protocol at the transport layer. Suggestions for integrating planned tactical systems to be GOSIP conformant are also presented which provide multicasting within subnetworks.

The DoD Network Management issue can be addressed by working within the standards groups to ensure DoD concerns such Management Information Base (MIB) objects are addressed. Additional security mechanisms are needed as well as a security profile and access control policy.

The Quality of Service (QoS) issue can be addressed by developing a program to establish a QoS framework and consistent QoS semantics. Until that is established, DoD should make best use of the existing mechanisms, allow providers to recover costs according to the level of service provided. The NIST Implementors Agreements provide a proposal for consistent semantics for the priority parameter. The tactical and real time needs are addressed by suggesting that negotiation of QoS parameters and a "thin" stack may solve these problems.

The Security issue can be addressed by appending a Security Profile to GOSIP that specifies the use of Secure Data Networking Program (SDNS)

components in a GOSIP conformant stack. We have developed a strawman security profile for all end systems requiring security. The Key Management Protocol (KMP) and the Security Profile (SP-3I) are recommended for all end systems requiring security. For additional levels of granularity the SP-4 protocol can be used to establish different security levels at the transport connection and the Message Security Protocol (MSP) can be used to provide additional granularity at the message level. The most significant challenge remains to develop a consistent, comprehensive access control policy.

The solutions to these military issues were often services made up of mechanisms distributed among several protocol layers. These solutions were gathered up into the appropriate protocol layer in section four to form the SPARTA recommended GOSIP supplement protocol stack. Each of these layers is summarized below:

- The physical layer (layer 1) has no additional recommended supplements.
- The Data link Layer (layer 2) should be expanded through additional protocols to support tactical needs for security, forward error detection/correction and spread spectrum techniques. Protocol augmentations such as a 32 bit checksum field (rather than 16) can significantly improve the data integrity for tactical systems. A suggestion is made to include existing tactical multicasting systems as subnets within the link layer.
- The network layer (layer 3) should be expanded with additional protocols to support a best effort multicast protocol, and security mechanisms.
- The transport layer (layer 4) should be augmented with additional technologies developed within the DoD Internet to give improved performance, a reliable multicast protocol that utilizes the previous best effort multicast protocol at the network layer, and security mechanisms.
- The session layer (layer 5) has the recommendation to use the unlimited data size option specified in version 2 of the ISO specification. In addition, the negotiation capabilities of the session layer can be expanded to provide QoS negotiation.
- The presentation layer (layer 6) has no additional recommended supplements.

- The application layer (layer 7) has recommendations for the use of security mechanisms and specifying optional features of the existing protocols.
  - The Mail Handling Service should be specified with the optional smart duplicating/splitting procedure to provide some multicast capability. In addition, where additional levels of granularity are needed, the MHS should use the Secure Data Networking System (SDNS) Message Security Protocol (MSP) combined with the Key Management Protocol (KMP) as specified by the security profile.
  - The File Transfer Access and Management (FTAM) and Virtual Terminal (VT) protocol need to have additional security mechanisms added to protect passwords and system access.
  - The Directory Service (DS) requires DoD participation in the DS standards bodies to address some security shortcomings. In addition, the SDNS KMP may require alternation to fit into the ISO plan for Key Management.

These recommendations should be studied, prototyped and evaluated, similar to the development of the DoD Internet protocols before committing them to standards. This approach is consistent with GOSIP since these recommendations can be considered tertiary sources. Most recommendations presented can be used by the commercial users to improve their communication protocols. Those DoD specific changes should be made with the philosophy that the change should be negotiated so that interoperability with commercial users is not precluded.

# 1. Introduction

The Assistant Secretary of Defense has mandated[1] the transition to the Open Systems Interconnection Protocols (OSI) as defined in the Government OSI Profile (GOSIP). This transition is intended to provide the government interoperability with the world wide standards for communication protocols and to benefit from the lower cost of off-the-shelf products which can be used for military use. These developments have been made possible by the stabilization of International Standards Organization (ISO) specifications and implementation of these communication protocols. It should be understood that this is an evolving process, the standards are updated and re-published every four years. The GOSIP specification allows this evolution by using primary, secondary and tertiary sources of information to specify the government communication protocols.

This technical report provides a set of recommendations that are intended to be used as tertiary sources of information which can be submitted to the standards organizations to become secondary and primary sources of information. The recommendations given in this report include suggestions for research areas, augmentations to existing protocols and the profiling of existing options. The recommendations are consistent with the evolutionary process by identifying near and far term actions necessary to provide the Department of Defense (DoD) with communication protocols meeting their mission objectives. The recommendations given should be investigated, prototyped and evaluated, similar to the effort used to develop the DoD Internet communication protocols. The results of this work should be entered into the standards bodies; Protocol Standards Technical Panel (PSTP), Internet Engineering Task Force (IETF), North Atlantic Treaty Organization (NATO), American National Standards Institute (ANSI), and ISO so that the GOSIP can specify the best communication protocols meeting the DoD needs.

## *1.1 Background*

In 1983, the NATO Tri-Service Group on Communications and Electronic Equipment (TSGCEE) Subgroup 9 (SG/9) on Data Processing and Distribution identified eight military features not addressed adequately by international standards bodies. These NATO Military

[1]Memorandum for Secretaries of the Military Departments, Chairman, Joint Chiefs of Staff, Directors, Defense Agencies, on Opens Systems Interconnection Protocols, dated 2 July 1987

Features describe high level military services expected to be incorporated into the international standards. Work in this area has progressed slowly over the past eight years.

The transition to the GOSIP protocols was mandated in a letter by the Assistant Secretary of Defense in July of 1987[2]. It directed the development of a transition strategy[3] and provided the first steps necessary to progress toward DoD OSI protocol implementations.

During 1989, the Defense Communication Agency convened its Protocol Standards Steering Group (PSSG) and Protocol Standards Technical Panel (PSTP) to address the technical suitability of ISO protocols for DoD use. In July, 1989, the PSTP met to reconsider the eight NATO Military Features. The result was to re-group the features into five broader "military issues". SPARTA has analyzed in a previous technical report[4] the NATO Military Features and the PSTP Military Issues noting the high level requirements driving these new communication protocol services . These high level requirements can be used to provide focus and direction for the network designers providing DoD implementations. The previous report also discussed each of the NATO Military Features and PSTP Military Issues to better understand the military needs.

### *1.2 Approach*

The approach taken in this report is to adopt the NATO Military Features and PSTP Military Issues as valid military needs and concentrate on developing communication services using underlying mechanisms to provide solutions to those military needs. We first examine the capability of the existing communication protocol standards to provide these services using available functions, then consider augmenting the protocols as needed and finally, if no immediate solution exists, we suggest further research areas. In each section we list the impact assessment for each of the military needs.

Next, we group the impact assessments made for the various services by protocol layer. Based upon this organization, we provide recommendations for DoD actions. We believe these recommendations to

---

[2] op.cit.

[3] The Department of Defense Open Systems Interconnection (OSI) Implementation Strategy, May 1988.

[4] SPARTA, Inc., "Review and Analysis of DoD Requirements for ISO Protocols," January 31, 1990.

be the best alternatives available at present. Nevertheless, they are presented as initial solutions from which stronger, more efficient solutions can emerge through analysis and prototyping.

### *1.3 Methodology*

The recommendations in this report have resulted from research focused on the requirements derivations from the NATO Military Features and PSTP Military Issues. Discussions in the PSTP's working groups on upper layers, lower layers and message handling protocols have also contributed to the recommendations. The PSTP chairman convened these three working groups beginning in mid-1989 in order to selectively attack pieces of the overall GOSIP technical assessment. Members of the working groups have considered both the military issues and the resulting protocol impacts. Experts have been invited to working group meetings to discuss specific protocol functions and capabilities and to provide additional insights into protocol impacts. The resulting recommendations have been made based upon a need to evolve from current GOSIP standards.

### *1.4 Organization of Report*

The remainder of this report is organized as follows. Section 2 presents the review and analyses of the military topics , in terms of services and mechanisms needed to support military data communications. Section 3 presents the recommended activities, grouped by protocol layers. Finally, section 4 presents the general conclusions of the report. Four appendices are included in the report for much more detailed analysis, they include discussions on Multi-Peer Data Transmission, Security, Message Handling System and File Transfer Access and Management .

## 2. Fundamental DoD Requirements

The list of military issues developed by NATO and later modified by the PSTP is a response to a number of more fundamental requirements. This section will review the motivation for the military features and the services necessary to provide these military topics. First, it describes the fundamental requirements that motivate each of the NATO service items. Then, it discusses fundamental requirements resulting from organization factors, especially the evolution of data communications in the US DoD up to the present.

### *2.1 Fundamental Requirements Behind the NATO Set*

The following paragraphs address each of the items from the NATO list of issues, pointing out the motivation for the item based upon military-specific required computer system and network attributes. This section provides a summary of a previous report[5] on military requirements and services. Expanded discussions are found in the previous report.

#### 2.1.1 Support for Mobile Hosts

Military data communications must be possible between hosts installed in mobile equipment (vehicles, aircraft, ships, etc.). Support for such hosts must enable service to be assured, despite this mobility. Access must be provided via physical connectivity to the network as well as logical connectivity via access control policy. In contrast, ISO protocols have been designed assuming fixed-plant operations and have no specific mechanisms to support end-system (host) mobility.

The underlying fundamental requirements are therefore assured service and access (and access control) supporting military communications in general and mobile end-systems in particular.

#### 2.1.2 Support for Multi-Homed Hosts

Military end-systems are frequently connected to more than one network access point, both in order to provide redundant access capabilities in the event of selective network failures, as well as to provide increased communication capacity between the host and the network.

The underlying fundamental requirements are therefore assured service in the face of anticipated threats to the networks, and increased

---

[5]SPARTA, Inc., op. cit.

performance and efficiency to be obtained from communication resources.

### 2.1.3 Multi-Peer Data Transmission

A large number of military messages must be received by multiple addressees. ISO protocols do provide means to accomplish this, but they are not efficient with respect to bandwidth or time. The underlying fundamental requirements are therefore performance and efficiency. There are some requirement areas that are addressed by having available a multi-peer data transmission service, such as assured service resulting from redundant message transmissions. However, the motivations behind a search for useful MPDT mechanisms are primarily performance and efficiency.

### 2.1.4 Support for Multiple Qualities of Service

Military messages have a variety of quality of service needs, in terms of timeliness of delivery, bandwidth required, reliability of delivery, etc. In theory, communication networks could be designed to meet the most stringent of these, but the cost would be prohibitive. Therefore, the underlying fundamental requirement is for performance and efficiency, as applied to messages with a wide variety of service needs.

### 2.1.5 Support for Network Management

Network management capabilities include the ability to monitor the status and performance of network entities, and the ability to perform some control actions. These capabilities will be used by network managers to identify diagnose, and correct problems more quickly, and they will likely support improved network performance. They will also assist in more positive management of network assets and to some extent network security. Therefore, the underlying fundamental requirements are assured service and performance and efficiency.

### 2.1.6 Security Services

Security services meet requirements to protect sensitive data from unauthorized disclosure, modification or destruction, and requirements to prevent unauthorized access to, or denial of service of organization and network resources. There are associated service to support general assurance, etc. Security services should be implemented in response to appropriate threat levels in order to meet a basic requirements to guard against those threats.

### 2.1.7 Support for Tactical Communications

Tactical communication systems must provide mobility, assured service and data integrity in an error prone environment. Performance and efficiency are important since the data throughput is typically less that 16K bits/second and the applications may include real time support such as fire control. The end systems are usually designed to be lightweight, battery powered. Confidentiality as well as low probability of detection/intercept is equally important for these military combat missions.

### 2.1.8 Support for Real-Time Systems

Real-time systems for military communications need fast services for critical messages, typically in a distributed (e.g., fire) control application including both measurement and control. These systems can be characterized by optimization of performance to meet the systems time requirements often at the expense of standardization or reliability of data communications. The underlying requirements for these services are performance and efficiency, similar to those for quality of service noted in Section 2.1.4 above.

### 2.1.9 Interoperability

Interoperability must be provided for existing systems as well as new systems developed by NATO allies. A combination of long system lifetimes, limited upgrades and maintenance budgets as well as custom designed communication solutions lengthens the transition to the OSI systems.

Tactical data communications users have typically developed their own solutions to meet their needs, as standards were lacking in the required time-frames; re-engineering applications and protocols using OSI will be a costly endeavor; there is a tendency to protect existing investments, especially as the existing solutions fit within the limited processing, power and bandwidth budgets typical of tactical equipments.

The US DoD and other NATO countries have become highly "inter-networked" via the TCP/IP protocol suite. US, UK and Scandinavia military organizations can all exchange mail, files and support remote login sessions via TCP/IP internetworking capabilities. More extensive inter-networking can be expected using an interoperable set of OSI standards. There are potential problems (such as different network layer services CONS vs. CLNS) that must be overcome by considering interoperability as a requirement.

Interoperability will continue to be a primary concern as protocols are implemented by many vendors and for many agencies with differing requirements. Custom mechanisms should be placed at lower layers and their effects shielded from the upper layers so that interoperability and cost savings from standard products are maximized. Custom systems can be integrated into the standards with gateways or conversion devices, however, new systems should try to adopt the new standards to optimize the future interoperability of these systems.

### *2.2 Requirements Summary*

The underlying requirements and organizational factors may be summarized as follows, with the paragraphs in which they are mentioned noted in parentheses:

1. Interoperability (2.1.9)
2. Assured Service (2.1.1, 2.1.2, 2.1.5, 2.1.7)
3. Access and access control (2.1.1, 2.1.6)
4. Performance and Efficiency (2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.7, 2.1.8)
5. Confidentiality (2.1.6, 2.1.7)
6. Integrity/authenticity (2.1.6, 2.1.7)

As can be seen from the number of references, performance and efficiency, and assured service are the two most important fundamental requirements.Despite their close association with the DoD, mechanisms used to satisfy these requirements should be useful for the commercial users as well.

## 3. Recommendations for Military Issues

This section provides our recommendations for the NATO Military Features and PSTP's set of Military Issues. These military topics have been investigated for alternatives and recommendations selected as appropriate. We have organized the sections to address the military topics as indicated below:

| Military topic | Corresponding section |
|---|---|
| NATO Military Features: | |
| Multi-Homed and Mobile Hosts | 3.1 |
| Multi-Endpoint Connections | 3.2 |
| Internetworking | 3.6, 3.7 |
| Network Management | 3.3 |
| Security | 3.6 |
| Robustness and Quality of Service | 3.4 |
| Precedence and Preemption | 3.5 |
| Real Time and Tactical | 3.2 |
| PSTP Military Issues: | |
| Multi-Homed Hosts | 3.1 |
| Multi-Peer Data Transmission | 3.2 |
| Network Management | 3.3 |
| Security | 3.6 |
| Quality of Service | 3.4 |

The following sub-sections address each of the military needs, providing a definition of the associated technical problems, background discussion on potential approaches for resolving the issues (i.e., solving the technical problems), and recommendations for near-term steps that should be taken toward resolution in the GOSIP context. Improvements to GOSIP protocols are examined that could be realized from experience with the DoD protocol suite. The subsections also discusses the potential impacts on GOSIP protocols that would be necessary in order to provide the necessary services to meet military needs.

## *3.1 Multi-Homed and Mobile End Systems*

### 3.1.1 Definition

Multi-Homed End Systems (MHES) and Mobile End Systems both use more than one network access point to send data to other end systems. The major difference between them is that MHES's typically use multiple access points to improve performance or provide improved survivability whereas MES's need access to the network resources. These characteristics can also be combined into a mobile host using more than one network access point to provide access, performance, and survivability. The overriding concern is that of transparency to the possible multiple data paths while operational.

MHES can have multiple (Sub) Network Points of Attachment (SNPA) and multiple Network Service Access Points (NSAP). The SNPA's provide connectivity to a subnetwork such as multiple IEEE802.3 adapters in a local area network (LAN) and are used to define a separate physical network connection. The NSAP's are used to define a service access point to a separate network protocol such as a dual protocol stack host containing a Connection Oriented Network Service (CONS) and a Connectionless Network Service (CLNS). Therefore, there are multiple ways to route data to MHES hosts from any other point in the network or internetwork. When an end-system uses multiple NSAPs, the routing both in the network and at other end-systems is more complex because it involves interaction with the intermediate routing entities. Services needed to support MHES are primarily routing and address resolution.

Mobile end systems (MESs) typically have a single NSAP but may also have multiple NSAPS if they must operate with other network protocols. The MES's differ from the MHES in that they physically move during their operation.

### 3.1.2 Background

MHES have existed in the DoD Internet as discussed in our previous technical report. These have typically been custom implementations since the closest thing to a standard has been implementation suggestions[6] rather than following an established standard. As discussed in our previous report, the implementations have suffered from static routing problems and have been unable to support dynamic load balancing or continuation of data streams broken during network

[6]J. Lekashman, "Multi-Homed Hosts in an IP Network", IDEA0019-00.TXT in the INTERNET-DRAFTS online directory.

failures. To meet the high level requirements for performance, survivability the GOSIP communication protocols must provide transparent dynamic load balancing.

Support for MESs is clearly a military requirement, because various tactical and operational end systems must be in motion, yet be highly available for communication with other end systems. On the other hand, the ISO protocols have been developed by a community of fixed-plant system users and so do not feature support mechanisms specifically for mobile end systems.

It is possible to achieve a good deal of support for MESs at the physical and link layers only. At the physical layer, use of radio and other radiative media directly supports end-system mobility, whereas use of fiber and wire media do not. Similarly, there are several link layer protocols that support mobile hosts, by enabling multiple access to the physical layer channel. Systems that exemplify these types of support include the following:

1. cellular mobile radio, which can support continuing connectivity between two end-points while one is mobile;
2. the INMARSAT mobile satellite system[7] provides connections between ship-board DTE and public data networks; such a DTE is inherently mobile within the satellite "footprint." The shipboard DTE uses X.25 protocols to exchange data with other end-systems via the satellite and other channels.

In addition, network architectures have been developed based upon shared radio communications. These include DARPA's Packet Radio Network[8] (PRNET) and the Survivable Radio Network[9] (SURAN). Developing these system required solutions to problems of limited sharing of radio channels, and routing in a dynamic topology. These solutions have been oriented toward operation within a closed (sub) network.

---

[7]CCITT, "Data Communication Networks: Interworking Between Networks, Mobile Data Transmission Systems," CCITT Recommendations X.300 - X.353, CCITT, Geneva, 1984.

[8]J. Jubin, J. Tornow, "The DARPA Packet Net Radio Protocols", Proceedings of the IEEE, Volume 75, No. 1, January, 1987, pp 21-32.

[9]N. Shacham, J. Westcott, "Future Directions in Packet Radio Architectures and Protocols", Proceedings of the IEEE, Volume 75, No. 1, January, 1987, pp 83-99.

Support for MESs in a network (or internetwork) using OSI protocols may involve one of two mechanisms: maintaining MES addresses (NSAPs) and requiring that the network compute new routes ("route change"), or requiring that the MES take on a new NSAP after it has moved ("address change"). In the latter case, the network uses its current computed routes, but the communicating end-systems associate new NSAPs with higher-level access point addresses.

There has been relatively little work to support MES at the network or higher protocol layer. However, one example experiment carried out by SRI used the Network Reconstitution Protocol[10]. It evaluated a technique of addressing based upon gateway rather than upon network association, and routing, based upon this addressing, performed by gateways. When MESs moved, their gateway affiliations and thus their addresses changed. Although the implementations performed correctly, the slowness was disappointing (address change response times on the order of minutes).

### 3.1.3 Issues

The major issue for support of MHES with the GOSIP protocols is to provide dynamic routing and to provide transparent load balancing among multiple routes. GOSIP version 1.0 provides only static routing, although future GOSIP's should support dynamic routing.

The ISO End-System to Intersystem (ES-IS) and Intersystem to Intersystem (IS-IS) routing protocols make use of dynamic routing to perform their functions[11]. The ES-IS protocol is normally resident on the MHES and provides the mapping of NSAP (network) and SNAP (sub-network) addresses to the intermediate (IS-IS) routers so that the data packets can arrive at the proper host interface[12]. While the IS-IS routing tables can support multiple NSAP entries (when NSAP is located in several overlapping routing areas), in order to support multi-homing, the IS-IS routing tables must also support duplicate NSAP entries for each independent path to the MHES. In addition, metric information is kept by the IS-IS routers on the path to a particular SNAP (network interface)

---

[10]SRI International, "Network Reconstitution Protocol," May 1986 (SRI Project 5453, Sponsored by DARPA, USAF Systems Command and Rome Air Development Center).

[11]P. Tsuchiya, "Components of OSI: IS-IS Intra-Domain Routing", Connections Magazine, October 1989, pages 40-45.

[12]R. Hagens, "Components of OSI: ES-IS Routing", Connections Magazine, October 1989, pages 46-51.

so the remaining interfaces would be used if one or more failed. There is a proposal to provide more information in the metrics so that better load balancing could be performed as opposed to simple link status (up/down), this effort should be supported by the DoD. Finally, an IS-IS redirect message can be used to redirect data traffic to a more optimal network path should a particular component fail (and another route exist). These are all normal functions of the ISO routing protocols.

The previous discussion provided a solution to a MHES where all interfaces existed on the same subnetwork. A similar solution exists for MHES where the network interfaces are connected to different IS-IS routers (not on a single subnetwork). The major difference would be the duplication of identical NSAP addresses in multiple areas. The IS-IS (level 2) routers must be able to support these duplicates in their routing tables. DoD needs to track the development of the IS-IS protocol to ensure the duplication of NSAP's in multiple areas is permitted in the developing standards.

The MES issues vary according to the user class considered. For example, link technologies such as radio and satellites have been used to permit the MES to use the same network access point. Transportable MES which move on a daily basis or longer may be supported using an address change approach where a new destination address is assigned and kept in a central location such as the Directory Service. Techniques such as Assured Destination Binding[13] can be used to facilitate this approach. For those mobile users physically moving between different network access point on more than a daily basis, the major issue is continuation of data streams. The address change approach defined below may not be able to respond faster than a daily basis considering the time required to update the Directory Service (network wide). Thus, the established data streams must be reconfigured when the end system moves fast enough to support the mobile end system across network access points. The ES-IS and IS-IS routing protocols provide all the basic services required of both MHES and MES systems using the route change approach. They need to be prototyped and evaluated for suitability.

The address-change approach and the route-change approach represent two alternatives for support of MESs in a broad internetwork environment. They can be generalized as follows:

---

[13]R. H. Stine, P. Tsuchiya, Assured Destination Binding: A Technique for Dynamic Address Binding, March 1987 (MITRE Corporation Report No. MTR 87W00050).

1. In the address change approach, an MES moves to a new physical location with a corresponding new NSAP address.

   The NSAP address for the unique network name is updated in the Directory Service. The basic requirement is for applications to obtain the current network address before attempting a network connection. This can be hidden from most applications by modifying the Association Control Service Entity (ACSE) to automatically query the Directory Service and obtaining the current network address. The speed of the Directory Update (network wide) determines the useful time constraints of this system. If the update process were fast enough, using techniques such as caching of Directory Service entries, this alternative may be able to support continuation of data streams (at the application level). The ACSE (or session protocol) could detect the loss of connectivity, query the Directory Service for the new address and attempt to re-establish connectivity. This alternative needs to be evaluated to determine the timing constraints to determine suitability.

2. In the route change approach, MES's use ES-IS and IS-IS routing protocols in a manner similar to the MHES. The ES-IS protocol "Hello" message is used to announces themselves, wherever they happen to be. The available network access points would be required to possess the IS-IS protocol, and update their routing tables to include these new hosts in their respective routing areas. An additional requirement for the MES would be a unique NSAP address to be used within the routing areas being traversed. This must be ensured so that duplicate NSAP addressed within a common area do not occur.

### 3.1.4 Recommendations

Broadcast link technologies, address change and route change approaches address the multi-homed and mobile host issues. The broadcast link technologies are in use today and provide solutions for limited mobility. The address change or route change technologies require prototyping and evaluation to determine their suitability for DoD's needs. The address change approach can be used as a transition

step until dynamic routing becomes available[14]. The route change approach makes use of capabilities designed into the routing protocols ES-IS and IS-IS to perform functions required by mobile and multi-homed hosts. The following general recommendations apply:

(1) for any mobile ES support basis, choose and standardize a physical layer. should be broadcast, probably radio or similar radiative media.

(2) support limited mobility via link layer solutions; ISO 8802 will support Mobile ES; other multi-access link layer protocols may also be useful.

(3) await evaluations of IS/IS routing prior to commitment to solutions for wide-ranging mobile hosts; trial implementations will be needed to measure and perhaps improve IS/IS routing update response; the alternative (address change) approach will need study also.

The address change approach makes use of the Association Control Service Entity (ACSE) and Directory Service to provide the current NSAP address of the destination end system. The Association Control Service Element (ACSE) can provide transparency to the application program. The disadvantage to this proposal is that continuous data streams cannot realistically be supported when the mobile end system relocates and a potential dead-lock exists if two mobile end systems relocate at the same time. The speed of update is very dependant on the update speed of the Directory Service. In addition, there are Directory Service Update authentication issues within X.509.

The dynamic routing approach makes use of the ES-IS and IS-IS protocols, which have capabilities that permit solutions for both the Multi-homed host and mobile host issues. They should be prototyped and evaluated before recommending modification to these protocols.. The ES-IS protocol hello function provides capability for both discovery and mapping of (sub) network points of attachment (SNPA's) and Network Service Access Points (NSAP). This information can be used by both end-systems and intermediate systems for dynamic routing purposes. The IS-IS Request Redirect function can be used to update the new delivery route for mobile system. The time constraints for this

[14]R. Perlman, "Internetworking with OSI," presented at INTEROP 89, San Jose, CA, December 1989. See also, P. Tsuchiya, "Components of OSI: IS-IS Introdomain Routing," Connexions, Oct. 89, pp. 40-45.

update process need to be evaluated to determine the suitability for DoD mobile subscribers.

There are several implementation recommendations when using dynamic routing. End systems should transmit hello packets not only for all NSAP's but also for all SNPA's. The implementation of the routing tables in both end systems (which listen to hello's) and intersystems must allow for multiple NSAP/SNPA pairs for a multi-homed host. The end system implementation of ES-IS should permit outgoing load balancing to be done within the end-system if multiple paths exist to a given network and the metrics associated with a path should be expanded to allow finer granularity.

## *3.2 Multi-addressing*

### 3.2.1 Definition

The NATO Military Feature Multi-addressing and the PSTP Military Issue Multi-Peer Data Transmission (MPDT) describe a military need to send duplicate data to multiple locations. It is a service addressing the performance/efficiency and assured service requirements. The service provides more efficient transmission of identical data to two or more destinations, conserving network bandwidth and reducing delays. In addition, it provides more reliability because data can be sent to both the primary and backup locations at the same time.

A service encompassing a superset of the DoD needs has been proposed within the ISO standards bodies as a Proposed Draft Addendum to the ISO Architecture Model (ISO 7498-1/PDAD2). Unfortunately, the proposed draft addendum has been terminated for lack of interest. An examination of the components of the addendum is useful to select the ones necessary to satisfy the DoD requirements. For the purposes of the discussions in this report, the following terminology will be used:

Broadcast Service - sending duplicate data every destination on network.

Multicast Service - sending duplicate data to a subset of every destination on network.

Unicast Service - sending data a single destination on the network.

In addition, these services can be implemented in a logical perspective using different physical mechanisms. For example, a logical multicast service can be made from a physical broadcast mechanism when combined with local filtering of the messages at each destination to sort out specific messages to a subset of the network.

Another point to consider is the management of the message transmission to the destinations. The message transmission can be implemented as a best effort or absolutely reliable basis. This can be compared to the tactical terminology for "action addresses" which must be acknowledged and "information addresses" which just get a copy of the message. The best effort message transmission requires no management of the message transmission and is the easiest to implement. The reliable message transmission requires varying degrees of management depending on the destination group dynamics. For example, one implementation of reliable message transmission may

require the speed of the transmission reduced to the slowest speed destination in order to ensure all the destinations get the messages reliably. More difficult problems can be created when some of the group members leave in the middle of the transmission, requiring rules for continuing the broadcast/multicast to the remaining group members. Some data transmissions may require both reliable and best effort transmissions (group contains action as well as information addresses). This group management function has been given the term Active Group Integrity. Because of these problems, reliable broadcast/multicast is still a research area.

A final point of information is the direction and control problems associated with the broadcast/multicast message transmission. There are two more terms to consider:

One to many - a single source and multiple destinations. This is the typical scenario when using multicast or broadcast transmissions.

Many to many - multiple sources and multiple destinations. Most examples degenerate into multicast and unicast situations, the best analogy is a vote taken within the group. Everyone in the group votes, a consensus can be reached, yet the votes of individuals are difficult to discern.

### 3.2.2 Motivation

The benefits to applications from MPDT services include reduction of bandwidth utilization and delay minimization, because transmissions of identical data do not have to be repeated. Most host computers have a finite limit on the number of simultaneous network connections they can support (e.g. SUN Microsystem workstations, which can support a maximum of 32 simultaneous connections). Applications that use such transmissions include various command and control systems (e.g., fire control), military message handling systems, distributed processing systems such as updating distributed databases, and teleconferencing systems. Examples of these applications as well as discussions of existing technology in this area are detailed in appendix A.

The ISO protocols as prescribed in GOSIP are oriented toward point-to-point communications and contain very little support for MPDT. The standards do support use of broadcast media, but they do not provide guidance on the construction of group addresses. Therefore, MPDT support has been identified as a military requirement area that is insufficiently addressed in ISO and GOSIP protocols. Nevertheless, there

has been a considerable amount of development work to realize MPDT services.

### 3.2.3 Mechanisms and Issues

The MPDT service can be implemented using mechanisms at various layers in the GOSIP protocol stack depending on the goals and resulting impacts desired. For example, a multi-addressing service already exists within the Message Handling Service using the smart splitting/duplication option described in appendix C. Current DoD Internet experimentation has been performed at the network layer and is described in RFC-1112[15]. Tactical systems such as the Maneuver Control System[16] (MCS) have provided this service at the lower layers. The following paragraphs discuss these efforts and their associated issues.

At the application layer, the 1988 X.400 Message Handling Systems (MHS) provides a capability to perform efficient distribution of a common message to multiple destinations via both address lists and group addresses if the smart duplication/splitting option is implemented within the Message Transfer Agent (MTA), a component of the MHS.

For multiply addressed messages, rather than making a copy of the message for each specified destination and routing them separately, the routing function is first applied to each destination address and then they are divided up according to their next 'hop' through the MTS. Copies of the message are made for each set generated, and the destination fields of the copies are assigned the corresponding list of addresses before forwarding. Each group address is associated with a specific MTA within the greater MTS. All messages addressed to a given group are forwarded to this MTA for destination list (DL) expansion (group address translation). When a message first arrives at an MTA, its destination field is examined and group addresses associated with that MTA are replaced by the equivalent address list. This process is then repeated until all nested group addresses are also expanded. Checks are made to prevent endless list expansion in the case of recursive address references.

---

[15] S. Deering, RFC-1112, Host Extensions for IP Multicasting. August 1989.

[16] "FY88 Army Command and Control Master Plan, Volume I, Concepts and Management," October, 1987.

The efficiency of this alternative is directly dependant on the number of destinations users shared by the MTA's. If every end user of the message were located off a single MTA, then no savings would result. However, this alternative provides the promise of some savings and is included in the specifications now. The MHS can also be used to distribute files by sending a binary message. Acquisition authorities need only to specify the smart splitting/duplication option to be implemented.

At the middle of the stack, there has been activity within the DoD Internet with respect to IP (network layer) multicasting. Internet Requests For Comments (RFCs) detailing host extensions for IP multicasting (RFC 1112) and a distance vector multicast routing protocol (RFC 1075) have been published and an experimental implementation is publicly available. IP multicasting provides a best effort multicast service at the network layer, using gateways to perform forwarding decisions based upon datagram group addresses. These techniques can be integrated into the CLNS due to its similarity with the Internet Protocol.

At the link layer, Hughes Network Systems has published a description of their broadcast service for use in X.25 point-to-point networks utilizing their integrated packet network hardware (IPN 9000). The basic operation of the scheme defined in our terminology is multicast and involves the use of X.121 addresses for groups of destinations, and the use of switches to provide both access to the multicast service and to act as multicast repeaters. The repeaters use standard point-to-point X.25 connections to pass data between themselves, and to deliver data to local destinations. From the perspective of the source, multicasts are point to multipoint, with return traffic via non-multicast X.25 connections. This scheme relies on a proprietary hardware and software implementation, similar to some of the tactical systems such as the Marine Tactical Data System rely upon the features of link-level ADCCP protocol for group addressing. A radio link can be shared by several stations that use a multi-drop protocol, such as ADCCP, to share the link. The ADCCP address field can be expanded and can allow group address definitions[17]. A scheme to fit existing tactical communications systems into the GOSIP architecture was introduced in the PSTP Lower Layer working group and is described in their Multicasting position paper. It offers the possibility for GOSIP compliance for some customized tactical communications systems by incorporating the entire system as a subnetwork and a link layer protocol. A thin GOSIP stack could be used between the existing

[17]D. E. Carlson, "Bit-Oriented Data Link Control Procedures," IEEE Trans. on Commun. COM-28(4): 455-467.

link layer protocol and the applications programs to provide an equivalent GOSIP stack. The multicasting features are enabled by interpreting an NSAP address as a group address and all multicasting done within the subnetwork. Although this approach is effective for closed tactical groups, it does not lend itself well to internet operation.

### 3.2.4 Impacts on GOSIP Protocol Layers

Layer 2 - Broadcast/Multicast efficiencies can be enhanced if maximum use of physical media is exercised . For example, the use of the ES-IS "hello" message is more efficient on physical broadcast type media such as IEEE 802.3 or HF radio networks. Additional protocols can fit into the OSI Architecture and should be added as appropriate.

Layer 3 - The GOSIP network layer can be enhanced with techniques available in the DoD Internet to support a best effort delivery multicast protocol.

Layer 4 - Research and develop reliable multicast. Several promising efforts are discussed in appendix A and should be used as a starting point.

Layer 7 - Implementation of the smart splitting/duplicating option for the DoD MHS MTA's as described in the X.411, Section Four, Procedures for Distributed Operation of the MTS, sections 14.3.1.4, 14.3.8, 14.3.10.

### 3.2.5 Recommendations

The termination of the PDAD 7498-2 MPDT addendum indicates a lack of interest for the full capabilities proposed. However, existing tactical systems make use of a subset of the MPDT components in non-standard protocols. MPDT solutions can be developed, but they will be one-of-a-kind until standards emerge. DoD can develop military standards which can be used by the Acquisition authorities as supplements to GOSIP until they can be processed by the standards bodies. We recommend two military standards be developed; a best effort multicast protocol, and a reliable multicast protocol. In addition, efficient implementations of the MTA using the optional smart duplicating/splitting feature should be specified in procurements.

The best effort multicast protocol can be prototyped within the GOSIP protocols at the network and link layers making use of existing techniques prototyped in the DoD Internet. The suitability of this protocol for use in different media's (broadcast vs. point-to-point) needs

to be evaluated and may require separate protocols at the link layer. The network layer components should be designed to accept different link layer protocols.

The reliable multicast protocol requires considerable research to be performed before is can be developed into a military standard. Some initial capability to satisfy existing DoD needs can be obtained by keeping the number of members within a multicasting group small ( < 64), the number of groups small ( < 16) and restricting the group dynamics allowed. The reliable multicasting protocol should make use of the best effort multicast protocol developed for the network and link layers and augment it with additional Active Group Integrity function at the transport layer. The connectionless transport protocol should be considered for possible augmentation since it should support a greater number of simultaneous connections with less overhead than the CLNS protocol.

The MHS MTA smart splitting/duplicating option can be required for all new MHS acquisitions if it is implemented from the 1988 X.400 specification. Future GOSIP specifications should use the 1988 X.400 specification.

## *3.3 Network Management Services*

### 3.3.1 Definition

Network management services provide the ability to perform management actions upon network equipment and software. The scope of such actions is just beginning to be defined, but they are the logical descendants of actions that can be performed from a system operator's console: starting and stopping devices and processes, allocating resources to tasks or to users, diagnosing faults, access to accounting data, access to audit data, etc. However, with the increasing use of both local and wide area networks, it is becoming necessary to perform many of these actions remotely. This means that a network manager or management process must be able to act from a single site to assess or change the status of network hardware and software components.

### 3.3.2 Background and Issues

Common network management services are needed to maintain DoD data communications networks and internetworks in a state of high availability and usefulness. It is especially challenging to manage network operations among heterogeneous hardware and software components, across a global scale as found in the current DoD Internet. Therefore, technically effective standards are needed for the definition and exchange of network management information. Fortunately, this area of standardization is being actively addressed in ISO and its contributing standards bodies such as ANSI.

The ISO network management standards include a management framework[18] (architecture), management information exchange protocols and services[19] (Common Management Information Service, Common Management Information Protocol: CMIS/CMIP) and a structure of management information[20] as well. In this framework, network entity status can be learned via CMIS "GET" primitives retrieving management information; network entity status can be altered via CMIS "SETs" on

---

[18]ISO/DP 7498-4, Information Processing Systems - Open Systems Interconnection - OSI Reference Model - Part 4: Management Framework.

[19]ISO 9595, "Common Management Information Services", and ISO 9596, "Common Management Information Protocol"

[20]ISO "Structure of Management Information," including ISO DP 10165-1 "Management Information Model"; ISO DP 10165-2 "Definition of Management Support Objects"; ISO DP 10165-3 "Definition of Management Attributes"; and ISO DP 10165-4 "Guidelines for the Definition of Managed Objects".

selected components or by CMIS-directed "M-ACTIONs". This is a very general framework in which it is possible to meet a broad spectrum of needs. We have concluded in an earlier technical report[21] that most DoD network management requirements can be met within this framework. However, in some areas DoD requirements do necessitate extension of the current developments. Access control is crucial for effective[22] network management. Current efforts do not specify access controls and mechanisms for their enforcement to the extent required for DoD. Mechanisms are needed to ensure the integrity and authenticity of data exchanged between network management processes -- managers, agents, clients and servers.

Similar to the elements of a shared database, access controls need to be enforced over some MIB elements. Most of the writeable elements need some protection in order to prevent denial of service. Still other readable elements may need to be shielded from universal access, if configuration data are sensitive. Unfortunately, these issues have been postponed by the NIST OSI Implementors' Workshop (OIW) Network Management Special Interest Group (NM SIG).

A means of authentication is required for access control policy enforcement. The claimed identity of a manager process seeking to write or read a MIB variable must be assured, before access is granted within the access control policy.

CMIS/CMIP Over TCP (CMOT)[23] is the IETF's second standard for performing remote management of protocol entities. (The IETF first such standard is SNMP[24].) The CMOT architecture provides for "thin stack" components to bridge between the application layer, where CMIS resides to the transport layer for TCP services. This "thin stack" strategy will facilitate migration to fully ISO networking from the TCP/IP networking protocols.

---

[21]SPARTA, Inc., "Network Management Identification of DoD Requirements and Evaluation of Current Developments," 31 January 1990.

[22]See section 3.5 and Appendix B, which discusses the security requirements for network management capabilities.

[23]Warrier, U. and Besaw, L., "The Common Management Information Services and Protocol over TCP/IP (CMOT); RFC 1095", April, 1989

[24]Case, J. D., Fedor, M., Schoffstall, M. and Davin, C., "A Simple Network Management Protocol (SNMP)," RFC 1098, April 1989.

Much of the standardization work in the past year, both within and outside of ISO groups, has been devoted to Management Information. This work is critical, because the definitions of the Management Information Base (MIB) elements determines what management capabilities are possible. To date, the IETF has developed the most advanced MIB versions, covering the physical, link, network, transport and selected higher layer protocols of the TCP/IP protocol suite. Relatively lesser progress has been made in defining standard management information for ISO protocols. Therefore, significant additional work is required before ISO networks could be managed to the degree that TCP/IP internetworks could be managed today.

The ISO management framework includes provisions for management outside of the scope afforded by CMIS/CMIP and by MIB elements. Layer Management Entities (LMEs) provide additional management services, transparently and autonomously. Routing functions may be regarded as network management performed through normal protocol operations and LMEs. Therefore, additional management issues will arise when the particular techniques used by LMEs are considered. For example, messages exchanged between LMEs will need authentication and other means for guarding against the spread of bad information through networks. Also, LMEs will need directory-like services to resolve information needs. This need will raise issues of the types of support that should be furnished: types of information available, policies for retaining versus discarding the information, etc.

### 3.3.3 Summary and Recommendations

ISO standards are now actively addressing network management, but have begun this only in the last two years. CMIS/CMIP will meet a majority of DoD needs. DoD needs that have not yet received attention in the standards groups include the application of access control and authentication, . The impacts of these requirements may be (1) need for DoD-specific managed objects to be included in the MIB (Management Information Base) and (2) development of security mechanisms -- authentication and access controls -- to support network management communications and applications.

In order to have its network management requirements represented in GOSIP and in resulting standard protocol software products, DoD should undertake research and development efforts. These efforts should be used to demonstrate methods for meeting DoD requirements and should be presented as the bases of updates to network management standards

in NIST working and special interest groups. Two major R&D areas are evident:

1. a program to identify and define MIB elements that will support DoD-specific network management applications; in particular, MIB elements for performance measurement and quality of service management in an OSI environment should be identified; such a program should make use of the development to date of MIB elements for non-OSI (i.e., TCP/IP) internetworking. This program should address management of all 7 protocol layers, in conjunction with concepts for network management
2. a program to identify security mechanisms to be used in conjunction with network management applications; the program should include defining security policies, identifying security mechanisms, both as system management applications and as layer management entities, and their roles in the management architecture, and identifying means for detection of and reaction to security events (e.g., audit collection and retrieval).

## *3.4 Quality of Service*

### 3.4.1 Definition

"Quality of Service" implies the ability to dictate to a network and receive from it services that give different characteristics of the communications channel with respect to averages and distributions such as delay, available throughput and bandwidth, and occurrence of errors. These are not the only parameters that may be affected by Quality of Services directives; confidentiality and related services (e.g., source authentication) could also be ordered via Quality of Service commands.

### 3.4.2 Background and Issues

Military network users depend on adequate performance and optimum efficiency; operations planners depend upon network support for a large number of users. Both planners and users require a wide dynamic range of operation in various environments. It would be costly to develop networks with a single class of service sufficient for the most demanding users, and it would be difficult to satisfy all user needs with a single class of service under limited costs. It is more realistic to assume for shared networks that several classes of service (and several associated costs) would be used to satisfy classes of users (high throughput, low delay, high reliability etc.).

The ability to select variable quality of service is a way to solve this problem. The more demanding quality of service can be supplied to a select class of users only. This potentially allows critical needs to be met without over-engineering a network. The multiple needs can be met by applying different mechanisms and resources to different classes of traffic. In addition, applications should not be required know details about lower layer functions, rather hierarchical classes of service should be considered which can be interpreted as appropriate at the various lower layers in the protocol stack.

Applications' differing quality of service requirements can be efficiently met by use or non-use of mechanisms such as Forward Error Correction Codes, Positive Acknowledgement Retransmission strategies, priority queueing, etc. These mechanisms are commonly employed in data communications systems. Matching applications to their lowest acceptable QoS via selection of mechanisms is usually the most efficient use of network resources. Furthermore, applications and end-users require a specific access method by which the required service quality can be requested from network services.

We summarize below the correspondence between the types of quality of service and the mechanisms commonly used in data communication systems. Also, we note the layer in which the mechanism is usually employed.

| Service Quality | Mechanism(s) | Layers |
|---|---|---|
| Low Delay | Routing | 2,3 |
| | Priority Sched'ing | Any of 2-7 |
| High Throughput | Routing | 1,2,3 |
| | Scheduling | 4-7 |
| Reliability | Coding Methods | 1 |
| | Error/Loss Det'n' and Correction | Typically in 2,3,4 |
| Security | Routing | 3 |
| | Anti-Jam | 1 |
| | COMPUSEC | 3,4,7 |
| | Message Prot'n | 2,3,4 or 6 |
| | Phys. Media Prot'n | 1 |
| Accurate Addressing | Name Service | 7 |
| | Checksumming | 2,3,4 |

This list illustrates where mechanisms may be employed, not where nor when they must be employed.

Interfaces to enable requests for different qualities of service currently exist in both the ISO protocols and in DoD's TCP/IP protocol suite. The interfaces are standard in the protocol definitions, but the actual implementations are not. For example, priority bits may be defined in packet headers, but the carrying network may not be capable of providing prioritized services.

The current set of ISO protocol standards does not support the requirement for Quality of Service that exists in military organizations (both the US DoD and NATO). More capabilities are needed to better match mechanisms and resources to applications and users. We list here some of the issues that underlie this generalization.

1. Lack of Comprehensive Quality of Service Framework A Quality of Service framework is needed to specify:
   - standard QoS parameters,
   - means for monitoring QoS and providing feedback to network management.
2. Lack of Common Measures of Quality of Service To date, Quality of Service at the network layer has been expressed in relative terms, such as preference for low cost over low delay. In the case of timeliness for some applications, this latitude may often be allowable; for real-time applications, however, less ambiguous definitions are needed. Similarly, the definitions of confidentiality should not be ambiguous.
3. Lack of Quality of Service Maintenance Techniques There are a great many ways in which networks can furnish requested quality of service (e.g., via specific routes). However, the availability of techniques is not uniform among networks and there no methods for dynamic application.

### 3.4.3 Recommendation

Although the current ISO standards provide definitions of quality of service, the actual implementations provide fewer classes of service and make their selection on a per-connection basis somewhat awkward. Therefore, DoD should proceed with efforts to enable network users to select from among several quality of service alternatives.

1. DoD should proceed with program to establish QoS Framework and consistent levels of service in an heterogeneous internetworking environment. Work on such a framework has begun in NATO and may serve as a useful basis. The framework purpose is to provide standard guidance with respect to monitoring quality of service and to management actions that can maintain quality of service.

   The program should address guidance for use of mechanisms in conjunction with particular selections of QoS. Active interchange is needed between groups developing internetwork routing schemes, groups developing network management systems, and users concerned with QoS.

2. In its procurements and developments, DoD should employ the existing QoS facilities in the ISO protocols to the fullest extent possible, in order to facilitate eventual implementations of QoS selections. DoD implementations of ISO protocols should carry complete QoS data fields, even though mechanisms may not be available to effect the actual QoS selections. DoD ISO protocol implementations should be capable of negotiating the QoS parameters in accordance with the ISO Session Layer Service Definition and Session Layer Protocol Specification.

3. DoD should proceed with efforts to enable service providers to recover costs in proportion to use (e.g., charge by packet volume). Furthermore, providers should be authorized to recover costs differentially according to selected Qualities of Service. This will allow charging at a higher rate for higher throughput, lower delay, or lower error rates. This will encourage providers to develop QoS selection and provision mechanisms.

4. DoD should manage user expectations with regard to quality of service, because it will take time for the necessary mechanisms to be widely implemented. Therefore, users should be advised to employ existing QoS parameters (throughput, priority, delay, security) as a guide to network provider, but also advised that actual service quality may vary with respect to:

   - Traffic Load
   - Routing algorithms and policies
   - Extent to which QoS mechanisms are implemented

### 3.5 *Precedence and Preemption (Priority)*

#### 3.5.1 Definition

There is a need in a military network to have precedence of (data) units to express the relative importance between the (data) units[25] during congested network operation. The terminology in this paper considers precedence and priority to be synonymous and be considered to be a Quality of Service (QoS) attribute of the data unit. Preemption is considered to be a mechanism used to provide distinction in the handling of different priority data units.

#### 3.5.2 Motivation

Both GOSIP version 1 and 2 specifications provide a priority parameter at each of the layers as referenced in the ISO specifications, however there are problems with the semantics of priority at each of the layers and preemption is stated to be a locally implemented QoS matter[26]. There exists different priority levels at nearly every layer, for example, Mail Handling Service (MHS) has three, Remote Operations Service Entity (ROSE) has eight, transport and network layers may have sixteen depending on which transport class or network protocol is used. In addition, there are priorities for establishing connections as well as the data units.

The DoD Internet has a precedence (priority) parameter which permits eight levels of priorities[27]. A mapping of these priority levels has recently been implemented in the DoD Internet at the X.25 level in the X.25 facility parameter field as shown below:

---

[25]NATO SG-9, Draft STANAG 4254, 15 February 1989.

[26]The Stable Implementor Agreements for Open Systems Interconnect Protocols, Version 2, Edition 3, Section 4.5.1

[27]MIL-STD-1777, Internet Protocol

| X.25 | IP Priorities |
|---|---|
| 11 -> | 111 Network Control |
| | 110 Internetwork Control |
| | 101 CRITIC/ECP |
| | 100 FLASH OVERRIDE |
| | 011 FLASH |
| 10 -> | 010 IMMEDIATE |
| 01 -> | 001 PRIORITY |
| 00 -> | 000 ROUTINE |

In a similar manner, the Stable Implementor Agreements for Open Systems Interconnect Protocols, version 2, edition 3, section 4.5.1.2.1 proposes four priority levels and maps them to an appropriate level or range of levels.

### 3.5.3 Recommendations

We believe the proposal to use three user priority levels; urgent, normal, non-urgent combined with a network management priority the best approach since it has been accepted by the commercial community and is not overly complex to implement. A research study can determine the proper mapping of military precedence (priority) levels to the three user levels as appropriate. We further propose that acquisition authorities specify that priority (and other QoS) parameter(s) be implemented according to the following proposal:

| Proposed GOSIP | | Military Priorities |
|---|---|---|
| Network | -> | Network Control |
| | -> | Internetwork Control |
| Urgent | -> | CRITIC/ECP |
| | -> | FLASH OVERRIDE |
| Normal | -> | FLASH |
| | -> | IMMEDIATE |
| Non-Urgent | -> | PRIORITY |
| | -> | ROUTINE |

The reserved Network Management priority level should be used only for network management (like the road shoulders use by emergency vehicles in a traffic jam). The six military precedence levels can still be preserved

at the application program level, but within the network the mapping into the three user levels is suggested.

For these priority levels to bear significance during network congestion, mechanisms (such as preemption) must be used to handle the network traffic. We propose the use of ordered queues to be used within the network components (gateways, routers) combined with a fair scheduling algorithm to provide fair handling of network traffic. The fair scheduling should evaluate the mechanisms such as preemption or simply using the time to live parameter to rid system of excess packets. In addition, the use of these priority levels must be administered with a policy similar to the one used in the DoD Internet to prevent abuse of the priority system. The details for the recommendations should be evaluated and more detailed recommendations made.

## *3.6 GOSIP Security*

### 3.6.1. Introduction

One of the attributes of DoD networking requirements is the need to incorporate security mechanisms and services throughout the network and protocol architecture. DoD networks must protect the information carried from unauthorized disclosure and from modification. These networks must also preserve the capability to deliver data in the presence of denial of service attacks.

These security properties are achieved through the integration of security mechanisms into protocols and network management functions, the incorporation of security devices, and the development of trusted components. To ensure interoperability, security must be a part of the specification of a networking profile for DoD systems intending to use OSI protocols.

A major issue for the DoD's use of OSI protocols is the definition, specification, and profiling of security approaches. As with other network services, the goal of a DoD OSI security profile is to specify approaches in sufficient detail so as to support secure interoperability. This requires the selection of specific mechanisms and algorithms and the specification of how those mechanisms are to be integrated. The DOD security profile must also address the options and choices in the protocol standards which impact security.

### 3.6.2 Security in the ISO Architecture

ISO 7498/2, Security Architecture provides common definitions of security services, presents alternatives for the placement of those services among the seven protocol layers, and discusses possible mechanisms. Figure 3.1 is taken from ISO 7498/2 and illustrates a matrix representation of the possible placement of security features in the OSI framework.

| | Layer | | | | | | |
|---|---|---|---|---|---|---|---|
| Service | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Peer Entity Auth. | o | o | Y | Y | o | o | Y |
| Data Origin Auth. | o | o | Y | Y | o | o | Y |
| Access Cntrl Serv | o | o | Y | Y | o | o | Y |
| Connection Conf. | Y | Y | Y | Y | o | Y | Y |
| Connect-less Conf | o | Y | Y | Y | o | Y | Y |
| Sel. Field Conf | o | o | o | o | o | Y | Y |
| Traff Flow Confid | Y | o | Y | o | o | o | Y |
| Connection Integ. with Recovery | o | o | o | Y | o | o | Y |
| Connection Integ. without Recovery | o | o | Y | o | o | o | Y |
| Selective Field Connection Integ | o | o | o | o | o | o | Y |
| Connect-less Integ Selective Field | o | o | Y | Y | o | o | Y |
| Conn-less Integ | o | o | o | o | o | o | Y |
| Non-repud. Origin | o | o | o | o | o | o | Y |
| Non-repud. Deliv. | o | o | o | o | o | o | Y |

Legend: Y Yes, services should be incorporated in the standards for the layer as a provider option.
o Not Provided

Figure 3-1 ISO 7498-2 Service Assignments

As discussed in Appendix B, the set of security services required to build trusted DoD networks are generally those enumerated for OSI as illustrated in Figure 3-1. Authentication, access control, data confidentiality, data integrity, and non-repudiation (as part of formal message and certain command and control applications) are all DoD security requirements. Not shown in Figure 3-1 but as discussed in ISO 7498/2, audit is also a requirement which permeates the OSI framework and therefore could not be placed in any separate layer. Given the ability for locating security services in multiple layers , the DOD Security Profile must define the exact placement of the services in order to insure secure interoperable standards.

### 3.6.3 Security Mechanisms for ISO

Once the security services have been specified the mechanisms for providing those services must be elaborated. One group that is working on developing those mechanisms is the protocol working group for Secure Data Network Service (SDNS). This working group is developing protocol specifications for some of the services identified in ISO 7498/2. The specifications that have been progressed the farthest are Security Protocol 3 (SP3), Security Protocol 4 (SP4), the Key Management Protocol (KMP), and the Message Security Protocol (MSP).

Conceptually, SP3 and SP4 are versions of the Security Protocol which are located between the transport and network layers in the OSI Reference Model. Integral to all of SDNS is the electronic key negotiation known as Firefly. During a Firefly exchange the two "terminals" exchange keying information and authenticity certificates. Each end system uses the union of the Firefly information to establish access control credentials and prepare the keys to be used for traffic encryption. The Security Protocol utilizes the generated keys for preforming the encryption and data integrity checks required of a particular protocol.

SP3 was designed and specified to provide those services ISO 7498/2 assigns to layer 3. Those services include Authentication (Peer Entity and Data Origin), Access Control, Confidentiality (Connection, Connectionless, and Traffic Flow) Connection Integrity without Recovery and Connectionless Integrity. SP3 utilizes the information transferred in the initial Firefly exchange to provide the authentication service. Access Control is provided by a mixture of local service and initial information obtained from the Key Management Center. In order to provide the Traffic Flow Confidentiality, SP3 can protect the classified address information in the SP3 encrypted header, while the packets traverse networks of lower security classification.

SP4 was designed and specified to provide those services ISO 7498/2 assigns to layer 4. Those services include Authentication (Peer Entity and Data Origin), Access Control, Confidentiality (Connection and Connectionless) and Connectionless Integrity. SP4 utilizes the information transferred in the initial Firefly exchange to provide the authentication service. Access Control is provided by a mixture of local service and initial information obtained from the Key Management Center.

Unlike the previous security protocols, KMP does not supply the end user with security services, but rather provides Key Management utility

services crucial to the correct operation of the other SDNS components. KMP is used between the Key Management Center and individual SDNS terminals for seed key conversion, electronic rekey, real-time Firefly exchange, and update of terminal traffic keys.

The SDNS MSP is an extension of CCITT recommendation X.400. The MSP resides at the mail user agent sublayer and assumes that the mail transfer agents are untrusted and therefore keeps the mail encrypted through any relays. MSP utilizes a staged Firefly exchange in lieu of the real-time Firefly exchange utilized in the other SDNS protocols. The staged approach utilizes a "public bulletin board" to publicize a part of the traffic key, which a sender will use in conjunction with his own private information to create the message traffic key. The recipient will utilize the senders public information, with the recipients private information to verify the key. MSP also supports multiple addressees by creating unique encrypting keys for each addressee. For DoD's purposes the "bulletin board" should not be "public" but additional information stored in the Directory Service Database, which will have its own access control policy.

As this brief examination of the SDNS protocol specification points out, the mechanisms to provide the ISO security services are being developed by the SDNS Protocol Working Group. Successful implementations of the specifications have been demonstrated. For DoD to benefit from this work, mechanisms such as these in support of the selected security services must be incorporated into a DoD Security Profile.. The next section suggests the initial input for such a DoD Security Profile.

### 3.6.4 DoD Security Profile

ISO 7498/2 and the current GOSIP specification leave flexibility in determining where security services are provided. DoD must utilize its experience with network security approaches such as BLACKER and the current work being done for the Defense Message System to develop a security profile. This profile must select the ISO layer(s) at which each security service is to be supplied. The profile must then be extended to select the appropriate mechanisms and supply all of the required parameter values in order to provide interoperable security solutions.

This document provides a recommended service layering as an initial consideration for the security profile. The definition of the parametric fields is specific to individual systems and while a major part of the GOSIP security profile is not presented in this document..

### 3.6.4.1. Security Service Assignments

#### Authentication

Authentication is used to inform the communicating entities of the identities of their peers. Placing the end system authentication at the application layer provides the finest granularity upon which access control decisions may be made. Authentication at the application layer is necessary to provide the end system with a means to protect its resources.

IS 7498-2 allows, optionally, the use of authentication at the transport layer. The provision of authentication at this layer may allow the simultaneous authentication of two or more session entities. While desirable, the granularity of authentication is only to the host transport entity (which is essentially the host system), so a secondary authentication will be required at the application to authenticate a user to the end system. Therefore, authentication at the transport layer does not appear to provide any advantages over provision at the application.

Subnetwork access is one of the major functions of the network layer defined by IS 7498-1, the OSI Basic Reference Model. To support the Subnetwork access role, authentication can be provided. Subnetwork access authentication may be useful in supporting mobile host applications where hosts dynamically join and leave subnetworks. Authentication at this level provides the network with a mechanism for the identification of users of its resources.

Authentication also needs to be provided as a part of all network management exchanges. These exchanges include CMIP activities as well as ES-IS and IS-IS exchanges.

#### Access control

Access control is tightly coupled with authentication. Access control decisions can be made based on information supplied by the authentication service to avoid masquerade and spoofing attacks. Given this tight coupling of access control and authentication, access control will be provided at the application and network layers.

#### Confidentiality

Confidentiality may be provided at the application layer where the intent is to limit access to the end user and his associated process. Confidentiality at the transport-network layer boundary, as discussed in Appendix B, limits access to end systems. Confidentiality services may

be employed at the link layer to prevent the disclosure of traffic flow information.

Integrity

Connection integrity with recovery is provided at the transport layer to protect from message sequence errors and data modification. Data integrity checks (for modification) are also performed as part of the SP processing coupled with cryptography, within management protocols, and within applications.

Data integrity checks are closely coupled with encrypting. A property of cryptography is that if a message is corrupted between encrypting and decryption, the received message will be unintelligible. Data integrity checks may be placed on either the encrypted message or on the plaintext message. In the first case, integrity checks are made prior to attempting to decrypt the message, in the latter the message is first decrypted and then checked.

Non-Repudiation

Non-repudiation is a service which is only related to application processing of communications. Non-repudiation services must be included in the application layer, to support applications such as Secure Message Processing and Secure Data Base Management. Such applications also have special requirements on the performance of other security services, such as authentication and access control, to insure the correct operation of the non-repudiation service.

3.6.4.2. Security Service Recommendations by Layer

Application Layer

The application layer will provide user authentication, data integrity, access control (including labeling), non-repudiation, and data confidentiality services. There are several mail related activities which have defined protocols that support these services. The Mail Security Protocol from the SDNS program and Privacy Enhanced Mail (RFC 1113-1115) are examples of application layer security approaches.

Presentation Layer

No security services are provided within this layer.

Session Layer

No security services are provided within this layer.

Transport Layer

Connection integrity with recovery, for connection-based information, such as sequencing and retransmissions, is provided within the transport layer protocol. Confidentiality, authentication, access control, and data integrity of message contents are provided by SP at the lower boundary of the transport layer.

Network Layer

Confidentiality, labeling, authentication, access control, and data integrity of message contents are provided by SP at the upper boundary of the network layer.

Link Layer

Data confidentiality may be provided at this layer to prevent traffic analytic attacks.

Physical Layer

No security services are provided at this layer.

3.6.4.3. Security Mechanism Recommendations

The recommended actions associated with those issues are as follows:

- Adopt the SP3-I option as the default DoD required capability. SP4 options may be employed between end systems which require additional security service. However, the default capabilities must always be accepted by all systems promoting widespread interoperability.
- Define the syntax and semantics for access control and labeling information to be included within management functions, directory requests, applications, and SP. Such definition will be taken from the SDNS access control concept with appropriate guidelines defined.
- Define the algorithm and format to be used for public key based authentication within management functions, directory exchanges, and applications.
- Include security capabilities within IS-IS protocols to be used within the DoD Internet. These security capabilities will need to prevent denial of service through exploiting router exchanges and support security based routing.
- Identify the cryptographic algorithms to be used within DoD OSI protocols. These definitions should be consistent with OSI algorithm registration although any actual registration would depend upon DoD policy decisions. Also design

standardized interfaces to cryptographic functions to support algorithm changes and easy incorporation of commercial protocol implementations.

- Adopt the Message Security Protocol for incorporations into all systems that require secure mail traffic.
- Address security for applications besides mail. Examine the work performed under the NCSC Internet Security Research program for directions to consider. Particularly the File Transfer Access Method (FTAM) and Virtual Terminal (VT) applications have security implications that must be resolved.

### 3.6.5 Summary

This section has examined the security facilities currently specified in the OSI framework. It has briefly discussed the ongoing work in SDNS Protocol Working Group. It justified the need for the creation and adoption of a detailed Security Profile as a supplement to GOSIP. The "strawman" Security Profile profile is meant to promote discussion and stimulate additional input into this area and not be the final profile that DoD should adopt.

## 4. DoD GOSIP Protocol Layer Supplemental Recommendations

This section provides specific recommendations DoD actions for enhancing and supplementing the GOSIP specified communication protocols and is intended to be used as a tertiary source of information. The actions include both development of positions for inclusion in a DoD GOSIP annex and development activities to resolve more complex protocol technical issues, to support further position development. The recommendations consist of three major areas; specifying options available with the primary sources but not GOSIP, augmenting existing protocols with tertiary specifications and identification of research areas where solutions do not exist today. These recommendations are then discussed in detail by protocol layer, rather than by military issue as in the previous section, in order to facilitate activity by protocol specialists.

Many of the recommendations deal with potential DoD supplements to the GOSIP specified set of communication protocols. These proposed supplements are intended to be validated by the DoD and presented to the standard groups in order that they become primary or secondary sources of communication protocols as specified by GOSIP.

When fully specified, the DoD supplements would introduce mechanisms and services within selected protocol layers to satisfy requirements as discussed in Section 2.

The technical recommendations that can be obtained by specifying the options available within the International Standards Organization (ISO) specifications (but not specified by GOSIP) are the

- Session Protocol Version 2,
- Message Handling System (MHS) smart splitting/duplication option,
- making use of the Quality of Service Parameters,
- adopting the NIST Priority Proposal, and
- making use of the Transport Protocol options.

The Session Protocol Version 2 allows unlimited data size negotiation, as opposed to limiting data size to 512 octets which can enhance the efficiency of communications channels. The MHS smart splitting/duplication option provides some limited multicast capability which can enhance the efficiency of mass message transmissions. Finally, the QoS parameters for priority, delay, throughput, security, error rate should be used to encourage vendors to implement

mechanisms that could enhance system operation. The semantics of the priority parameter can be standardized by accepting the NIST Implementor Agreements proposal on consistent levels of priority within the end systems. The use of the extended transport protocol options in conjunction with the Session protocol version two allow much greater efficiencies with high speed networking. These improvements can be obtained by specifying existing options to the ISO specifications by acquisition authorities in future procurements.

The next area of technical recommendations consist of modifications of existing protocols. The recommendations include the implementation of the advanced technology for congestion avoidance, best effort multicast and other extensions to the transport layer protocol, developing a security profile to specify the use of Secure Data Networking System (SDNS) mechanisms, using a "thin" protocol stack and extending the 16 bit checksum to 32 bits in the link layer protocol. The extensions to the transport protocol make use of advanced technology developed within the DoD Internet and integrate it with the GOSIP transport layer protocol to give more efficient operation. The development of a security profile is necessary to assist acquisition authorities the proper placement of SDNS mechanisms and specifying an adequate access control policy. The thin protocol stacks are a minimum subset of the GOSIP protocol stack to provide access to dumb network components (modems) and to provide better service for tactical and real time users to reduce system overhead. The 32 bit checksum extension should provide better data integrity at a minimal increase in the parameter field width and is already in use in some of the link layer protocols. These changes require some modification of the existing protocol standards and evaluation before changing the standards.

The final area of technical recommendations are the identification of research areas that need to be developed further before recommending a specific solution to the DoD communication needs. These areas include the research and development of a QoS framework so that network users can specify and receive (and be charged) specific communications channel characteristics that are necessary for there missions. Another area requiring further research is the development of a reliable multicast protocol that can provide service to a dynamic group.

These recommendations are discussed by protocol layer in the following sections.

### *4.1 Physical Layer (Layer 1).*

Physical layer entities perform electrical encoding and decoding of the data for transmission over a medium and regulate access to the physical network.

#### 4.1.1 Physical Layer Impacts

Different physical interface standards are required according to data rates and cabling distances, network topologies and other operational factors (e.g., security). However, GOSIP version 2.0 does not mandate specific physical layer standards. Therefore, DoD-specific requirements for physical layer implementations and interface standards create no current impact to the GOSIP.

#### 4.1.2 Recommendation

Acquisition authorities should continue procurements using the current standards (MIL-STD-188, IEEE 802, RS-232, RS-422, FDDI, etc.) as necessary to meet current requirements. Acquisition authorities should also stay abreast of further developments of physical transmission technology to maximize opportunities for increased system performance and reliability.

### *4.2 Data Link Layer (Layer 2).*

The data link layer performs frame formatting, error checking, addressing, and other functions (such as error correction) necessary to ensure accurate data transmission between adjacent systems. GOSIP allows a choice among several data link layer protocols; 1) High Level Data Link Control (HDLC) Link Access Procedure B (LAPB), in conjunction with X.25; 2) ISO 8802/2 in conjunction with ISO 8802/3, ISO 8802/4 or ISO 8802/5; and 3) Q.921 for operation on ISDN B channels. Acquisition authorities' choices will depend upon the communications media available, topology needed and other factors specific to the end system environment.

#### 4.2.1 Data link Layer Impacts

The GOSIP choices among data link protocols are overly restrictive and do not allow many primary DoD requirements to be met. Link layer protocols do exist to support MPDT and secure communication (LPI, LPJ), but they are not included in GOSIP. The impact of DoD's requirements in the data link layer is to broaden the range of allowable

link layer protocols beyond GOSIP. Link layer protocols supporting techniques for forward error correction, spread spectrum, and MPDT should also be a part of GOSIP.

Protocol implementations will also need to be expanded to accommodate network management requirements. This will include accumulating statistics for errors and data units passed, and reporting interface state information.

### 4.2.2 Data Link Layer Recommendations

DoD should develop within its own GOSIP profile an expanded list of link level protocols, to includes ones that support MPDT, security and other requirements in present systems. We propose the expansion of the current 16 bit checksum field to 32 bits to provide additional data integrity for tactical applications. These and other changes can be made to an existing protocol such as X.25 layer 2 or combined into a new protocol. This would make it easier for a wide variety of tactical and other systems to both meet their operational requirements and be GOSIP-compliant.

We propose a development effort to standardize advanced link technologies such as Forward Error Correction in addition to error detection in order to promote interoperability. The development of standardized Forward Error Correction should permit negotiation to select a compatible scheme to be used, and turned off when not required.

We propose a similar development effort to standardize spread spectrum techniques/mechanisms to promote interoperability. This may be accomplished through a comprehensive security profile. Commercial spread spectrum techniques were legalized in 1985 when the Federal Communications Commission (FCC) promulgated rules to authorize its use.[28] Two standards are currently competing for acceptance among European Community nations; British Telecommunications developed Cordless Telephone 2 (CT-2) specification; the Institute of Electrical Electronics Engineers, the 802.4L committee is devoted to wireless token-bus access. These would be good starting places.

In the area of Network Management, MIB elements unique to DoD for the data link layer should be defined and followed in NIST and IETF MIB standards activities.

---

[28]Network World, An IDG Communications Publication, Volume 6, Number 44, dated November 6, 1989, page 74.

### *4.3 Network Layer (Layer 3).*

Layer 3 is concerned with moving data units from their source to the destination, choosing paths through the interconnecting networks. It is the lowest layer that deals with end-to-end transmission. Additional service, such as flow and congestion control may be provided.

#### 4.3.1 Network Layer Impacts

Impacts to the network layer arise primarily from the requirements for improved performance and efficiency of the network and from needs for assured service.

1. The network layer as dictated in GOSIP must be expanded to include multicasting services and expansion of the metrics maintained by the routing protocols. These will support efficient use of network bandwidth and load balancing of network paths.
2. Network layer implementations will also need to be expanded to accommodate network management requirements, as noted for the data link layer. This will include accumulating statistics of errors and data units passed and reporting and setting status. The management of Intermediate Systems will need improvement and expansion to assure adequate network routing performance and to support mobile/transient users. Network layer implementations will need to be expanded to accommodate security mechanisms as mandated in the security architecture.

#### 4.3.2 Recommendations for the Network Layer

1. We recommend that existing multicasting techniques (furnishing best-effort delivery only) developed for use within the DoD Internet[29] and tactical systems be prototyped and evaluated as extensions of GOSIP protocols.
2. The MIB elements for the network layer should be defined and DoD should follow these efforts in NIST and IETF MIB standards activities. A security profile should be developed to select security mechanisms as defined in section 3.6

[29]S. Deering, "Multicast Routing in Internetworks and Extended LANs", SIGCOMM Summer 1988 Proceedings, August 1988 and Crowcroft J., Paliwoda K., "A Multicast Transport Protocol", SIGCOMM Summer 1988 Proceedings, August 1988

### *4.4 Transport Layer (Layer 4).*

Layer 4 provides reliable, transparent, end-to-end transfer of data. The transport layer entities optimize the available network services to provide the performance required by each session entity. Optimization is constrained by the overall demands of concurrent session entities and by the quality and capacity of the network services available to the transport layer entities. Transport connections have end-to-end significance, where the ends are defined as corresponding session entities. Transport protocols regulate flow, detect and correct errors, and multiplex data, on an end-to-end basis.

#### 4.4.1 Transport Layer Impacts

The ISO transport layer standards offer protocol classes capable of providing the service currently offered by DoD's TCP. Therefore, there are no major impacts upon the ISO transport layer resulting from DoD requirements. However, many have pointed out that ISO transport protocol implementations lack the maturity present in TCP implementations, because of the longer experience with the latter. Applying the lessons learned from TCP has been advocated for ISO TP-4[30]. Our recommendations for improvements to the ISO transport layer are made in this same spirit.

The transport layer supplements to improve security are defined in a comprehensive security profile. The network management objects need to be defined and monitored within the standards process to ensure their suitability for DoD.

#### 4.4.2 Transport Layer Recommendations

Advanced technologies developed for the DoD Internet should be integrated into GOSIP Transport Protocol Class 4 (TP-4). The features most applicable include; the use of extended formats, adaptive congestion control, unlimited window size, extended window granularity, and moving checksum field to end of packet. It should be noted that the graceful close function provided by TCP can be approximated using session layer graceful release capability.

---

[30]D. M. Piscitello, Presentation at INTEROP 89, San Jose, CA, "TCP and TP-4".

The extended formats for sequence space, flow control credit[31] and initial sequence number allows much more data to be in transit, such as a satellite channel, before a wrap-around of sequence numbers occurs. By combining the extended formats with a non-zero initial sequence number, the possibility of sequence number overlap between multiple transport connections can be minimized.

The adaptive congestion control mechanisms developed recently for the DoD Internet TCP[32] should be incorporated into the TP-4 protocol to improve the efficiency of networks. Military use of networks becomes more crucial during crisis times, typically when network congestion is the greatest.

The use of negotiated maximum protocol data unit and window sizes permits efficient use of very high speed networks over long distances, such as satellite channels. The larger protocol data units permit more efficient network operation because it reduces the amount of acknowledgments and their associated propagation delays for a given data transmission. Rather than use a larger size than is currently specified, the size should be negotiated to allow future upgrades without changing the specification.

The granularity of window size should be modified to allow sizes other than modulo 2. This will permit finer adjustments than is currently permitted.

A negotiated option to move the checksum parameter to the end of the protocol data unit will permit more efficient operation for extremely large PDU's and permit very fast operation. This change does not require the entire PDU to be located in the host computers memory in order to calculate the checksum and allows large PDU lengths. An additional benefit is the applicability of using hardware to speedup the checksumming process.[33]

DoD should research reliable multicasting techniques to allow a reliable multicast at the transport layer. The reliable multicasting should make

---

[31] Request for Comments: 1007, Military Supplement to the ISO Transport Protocol, Wayne McCoy, 1987, section 4.3.1.a, page 9.

[32] V. Jacobson, "Congestion Avoidance and Control," Computer Communications Review 18(4): 314-321 (August, 1988).

[33] R. Beach, Presentation at INTEROP89, San Jose, Ca., "Implementing TP4 on Gigabit Networks".

use of best effort multicast protocol implemented at the network layer and augment it with the retransmission, sequencing capability and group management function of a new or augmented protocol such as the connectionless transport protocol. Restricting the range of allowed group dynamics may simplify near term solutions.

DoD should proceed with a Quality of Service definition and framework program, to identify a consistent layer interface to enable service quality requests and diagnostic feedback to be passed between layers.

DoD should develop a general security profile to select the appropriate security mechanisms used in GOSIP. A preliminary recommendation is to use the SDNS SP-3I protocol for all secure hosts and augment the security as needed with SP-4 to provide superencryption where needed. These security components require the SDNS KMP and overall access control policy defined.

In the area of Network Management, DoD needs to define and track the MIB elements in standards bodies (IETF and NIST) to ensure they provide the DoD requirements.

### *4.5 Session Layer (Layer 5).*

Layer 5 provides for the orderly exchange between presentation entities. To transfer the data, session connections use transport connections, During a session, session services are used by application entities to regulate dialogue by ensuring an orderly message exchange on the session connection. There are currently two version of the session layer protocol, the major difference being the maximum data unit size; 512 octets for version 1, unlimited size for version 2.

#### 4.5.1 Session Layer Impacts

The impact of DoD requirements upon the session layer, as specified by ISO and by GOSIP is only slight. Current DoD applications use TCP connection management services to perform only a subset of the services offered by the ISO session layer. The ISO session layer negotiation capability, as applied to session's Quality of Service, is an important service.

#### 4.5.2 Session Layer Recommendations

DoD's profile for the session layer should explicitly state that the full extent of such negotiation capability.

We recommend version two of the session layer which provides an unlimited data unit size negotiation capability. This will allow larger data units to be exchanged over high speed networks and may increase overall efficiency. The session layer impacts involve upgrades to allow more negotiation capability, with semantics of the options defined, and adherence to the security profile.

The session layer negotiation capability should be prototyped and evaluated for its consistence with an overall Quality of Service definition and framework. Additions to the existing options may be required to request lower layer services such as multicasting. The Quality of Service measures and measurement techniques require semantic definition in order to be useful network wide. In addition, the selection of a reduced set of session function could be used as a lightweight session protocol to users requiring only a graceful close capability.

### *4.6 Presentation Layer (Layer 6).*

Layer 6 provides for the representation of information. The presentation layer provides the representation of: 1) data transferred between application entities, 2) the data structure that the application entities use, and 3) operations on the data's structure. The presentation layer is concerned only with the syntax of the transferred data. The data's meaning is known only to the application entities, and not to the presentation layer.

#### 4.6.1 Presentation Layer Impacts

The impact of DoD requirements upon the presentation layer, as specified by ISO and by GOSIP, is only slight. Current DoD applications use the ASCII data and binary octet data definitions for presentation standards (i.e., in message and file exchanges). In most cases, presentation layer functions have been developed as adjuncts to the file transfer, message transfer and virtual terminal protocols. In other words, DoD applications current use only a subset of available ISO presentation layer functions. In fact, concerns exist as to the

performance penalty associated with a layer whose functions are not in demand[34].

#### 4.6.2 Presentation Layer Recommendations

DoD should investigate the utility of lightweight presentation protocol implementations. These may offer a low cost interim solution for layer 6, provided that they can interoperate with fully compliant session layer implementations and that they provide sufficient performance. If so, then the lightweight presentation protocol should be included in DoD's profile of the session layer.

### *4.7 Application Layer (Layer 7).*

Layer 7 provides services to the application process. Functions satisfying particular user requirements are contained in this layer. Representation and transfer of information necessary to communicate between applications are the responsibility of the lower layers.

#### 4.7.1 Application Layer Impacts

There will be multiple impact areas from DoD requirements and issues upon the application layer, because there are multiple services within the application layer. There are currently three Application Service Elements (ASEs); more will be added, possibly in conjunction with a security architecture. Therefore, inclusion of security mechanisms will be a major impact area in layer 7. Layer 7 also includes major service protocols such as FTAM and MHS. As these protocols evolve to accommodate DoD requirements, further impacts will be realized in layer 7.

#### 4.7.2 Application Layer Recommendations

The application layer recommendations consist of specifying options within existing protocols, augmenting others to address security concerns and to support mobile users. The first recommendation already exists within the 1988 ISO MHS specifications. DoD Mail Handling Systems should implement the Message Transfer Agent message splitting/duplication function to permit economy in bandwidth and time savings.

---

[34]Rose, M., The Open Book. A Practical Perspective on OSI (Prentice-Hall, Englewood Cliffs, NJ, 1990), pp. 142-143.

DoD should augment existing protocols and add additional security protocols to address security concerns. The File Transfer And Management (FTAM) and Virtual Terminal (VT) protocols may require augmentation to address security concerns about password protection. The Directory Service (X.509) should be upgraded to provide additional authentication services. Additional security protocols should be added such as the Message Security Protocol (MSP) and Key Management Protocol (KMP).

DoD should proceed to define addenda and profiles to be applied to directory services so as to support Multi-Homed End Systems and Mobile/Transportable End Systems until dynamic addressing is available within GOSIP. This changes include a secure update capability for Directory Service and modification of ACSE to support Directory Service Query to obtain the current network address transparent to the application program.

DoD should develop program designating a central registration/naming authority. This is especially important to provide unique NSAP addresses given to mobile hosts.

Specific recommendation details concerning the MHS and FTAM protocols are given in appendices C and D respectively.

## 5.0 Conclusions

This technical report has provided recommendations for the enhancement of GOSIP and GOSIP protocols to meet DoD requirements. These recommendations were presented both according to a set of military issues and according to the affected protocol layers. The recommendations encompass both longer-range and immediate activities. We have identified areas requiring further research, augmentations to protocols and specification of existing protocol options to meet Military communications needs. These recommendations are intended to lead to tertiary sources of information, consistent with GOSIP, and to provide input to the evolutionary development of the communication protocols. The recommendations that are suitable should be entered into the standards bodies to become secondary and primary sources of information.

The recommendations are made in advance of the implementation and deployment experience that are necessary for sound standards. These recommendations should be investigated, prototyped and evaluated as to their suitability for satisfying DoD needs. Based on this experience, implementation notes should be developed to provide guidance for improved implementations.

The scope of the recommendations exceeds the resources and manpower currently available in the DCA. Therefore, many organizations, including contractors must be called upon for specific contributions. DCA should follow these activities and continue participation in national forums such as the IETF and the NIST OSI Implementors' workshops. These groups produce RFCs and Implementors' agreements which become GOSIP secondary information sources.

On the whole, GOSIP protocols can meet the requirements of many or most DoD network subscribers and Open System users. DoD and its major services have developed GOSIP transition plans to guide them from the current use of TCP/IP protocols to procurement and use of GOSIP protocols. Even though this report concentrates on areas where GOSIP protocols do not meet military needs, its position is that the transition to GOSIP protocols should and will proceed. The recommendations made are intended to improve the protocols to better serve the DoD needs. Most of these improvements address the performance and efficiency of these protocols and can be used by the commercial users and integrated into the international standards so that the interoperability and cost savings can benefit all. Where there is no foreseen commercial interest in a DoD specific modification, use should

be negotiated so that interoperation with commercial users is still possible while meeting the DoD's needs.

## Appendix A: Multi-Peer Data Transmission

This appendix provides more detailed information on Multi-Peer Data Transmission (MPDT) which is a broader term than the multi-addressing discussed in section 3.2.

### *A-1 Multi-Peer Data Transmission Summary*

Multi-Peer Data Transmission (MPDT) is the transmission of identical data units or messages to one or more destinations. While this transmission may be reliable or unreliable, the primary purpose of MPDT is to realize bandwidth and delay savings by taking advantage of networks utilizing inherently broadcast mediums. Secondary features include coordinating multi-party connections or conversations on such networks, and to provide these capabilities to inherently non-broadcast networks. MPDT is of interest to the DoD as it is a means to satisfy performance requirements related to bandwidth utilization and timeliness of delivery. In addition, MPDT can be used enhance survivability by allowing systems to send identical information to multiple back-up sites in a manner more efficient than traditional one-to-one communication can provide. Unfortunately, the current ISO/OSI protocols have limited MPDT capabilities which will not be expanded in the near term.

At present, only the Message Handling Service (MHS) provides a multi-peer addressing capability[1], while a proposed draft addendum to expand the OSI reference model[2] to provide more general multi-peer capabilities was recently dropped. While MPDT requirements for DoD messaging systems may be met by properly profiling the MHS, a number of other applications' needs are still unmet (teleconferencing, packet voice, tactical communications, to name a few), and their requirements (efficient bandwidth utilization with low delay, and reliability where needed) persist, though standards seem far off.

Fortunately, there has been promising research in the TCP/IP community with Internet multicasting that may be readily applicable to the OSI environment [3]. While this work does not cover all aspects of

[1]"Message Transfer System: Abstract Service Definition and Procedures", (CCITT X.411 / ISO DIS8883-1), November 1987

[2]Draft Addendum to ISO 7498-1 on Multi-peer Data Transmission, International Standards Organization (ISO), November 1988

[3]S. Deering, RFC-1112, Host Extensions for IP Multicasting, August 1989.

MPDT, it does provide a starting point along with a low level MPDT capability - unreliable multicast of datagrams. This will provide a baseline multi-peer capability upon which research into more difficult areas of MPDT can be built (such as providing reliable communication using multi-endpoint connections.)

*A-2 MPDT Background*

This section is presented to bring the reader up to date on the current status of MPDT in the commercial, standards and research communities. Terms are defined to clarify the discussion, DoD requirements are reviewed, and work to date in this area is discussed.

### A-2.1 MPDT Definition of Terms

Multi-Peer Data Transmission (MPDT) is the transmission of a data unit to one or more destinations. Below are terms commonly associated with MPDT along with their definitions for the purposes of this discussion.

Broadcasting - sending information to all stations on a network.[4]

Multicasting - directed broadcasting of information to selected end destinations on a network.

Unicasting - special case of multicasting, where the number of destinations is one.

Physical broadcast/multicast - a broadcast on a network that utilizes a medium that is inherently one to many in nature (e.g. radio, satellite, IEEE802.3).

Logical broadcast/multicast - a broadcast on a network that utilizes a medium that is NOT inherently one to many in nature (e.g. point-to-point networks), and thus requires simulation of a physical broadcast via multiple transmissions of the same data thru additional hardware and/or software.

Unreliable broadcast/multicast - the broadcast/multicast transmission of data on a "best efforts" basis. That is, while in most cases data should be transmitted successfully, there are no guarantees as to the integrity of messages' contents, their ordering, or actual delivery.

Reliable broadcast/multicast - the broadcast/multicast transmission of data that is guaranteed to be accurately

[4]P. Blankenship, "Minutes: PSTP Working Group 1 Lower Layers Protocols Meeting on 12 December 1989", 22 December 1989

received by all destinations. Additional reliability features include preservation of message ordering and notification of the sender upon message receipt by the destination.

Multi-Endpoint Connection - an association among two or more peer entities for the transfer of data. Two types of multi-endpoint connections have been defined - centralized, and decentralized. In a centralized connection, data sent by the entity associated with the central connection end-point is received by all other entities, while all other transmissions are received only by the central entity. In decentralized connections, all entities receive all transmissions[5]. While multi-endpoint connections may be reliable or unreliable, they are most commonly associated with reliable transmissions and the associated overhead functions and mechanisms to manage such connections, such as maintaining acknowledgement windows and timeout counters.

With respect to the above terms, while multicasting may be reliable or unreliable, it is most commonly associated with unreliable datagram services. Similarly, multicasting is most commonly associated with physical broadcast based networks though this capability can be logically provided to some extent on point-to-point networks as well. In the greater context of MPDT however, the goal is to make the best use of all available mechanisms and physical network capabilities to realize performance gains and/or resource savings.

### A-2.2 MPDT To Improve Network Performance

In addition to the above, the use of MPDT is expected to help networks satisfy DoD requirements for bandwidth utilization and delay minimization, and support other requirements (such as reliability) where needed in doing so. For example, mechanisms that enhance communication between multiple sites will help to support systems whose survivability depends on delivery of duplicate information to multiple backup locations.

Below we discuss a number of applications whose utilization of network resources could be greatly enhanced through the use of MPDT, making them more suitable for DoD use.

---

[5]ISO 7498-1 Open Systems Interconnect (OSI) Basic Reference Model

### A-2.2.1 MPDT Tactical Communications

The DoD has a number of specialized applications whose needs are unique with respect to bandwidth utilization and delay performance. The characteristics of the tactical environment are such that bandwidth conservation and low delay are more than simply desirable as a means of cost savings - they are absolute requirements.

Tactical systems need to send information such as tracking and fire control data to multiple locations in an environment where communications resources are usually scarce, and likely under attack. As data rate reduction is one of the more common countermeasures (or side effect of such countermeasures) to jamming, bandwidth is at a premium. Data rates of 75 bits per second (bps) are not unheard of. In addition to dealing with little available bandwidth, these systems usually carry time sensitive data (such as target tracking information), requiring minimal delivery time. Customized networks and applications designed for tactical use often cannot work with one another due to differing technical approaches taken in trying to meet the needs of this demanding environment. Standard MPDT services or means of access would ease the problem of incompatible systems.

Tactical applications make use of both reliable and unreliable service. Tracking systems typically transmit position updates frequently enough to tolerate an occasional lost or damaged packet or two, while fire control messages need assured delivery and must maintain data integrity.

### A-2.2.2 MPDT Electronic Mail

Almost all electronic mail (E-mail) applications provide their users with the ability to send a given message to more than one addressee. Typically though, the application carries this out by actually sending a separate copy of the message to each individual destination, causing the load on the network to increase in direct proportion to the number of addressees. Some E-mail applications provide mail 'exploders' that will deliver the same message to multiple local users once it has reached a given end system. This scheme is useful, but only where there is more than one intended recipient at the host implementing the exploder function. In the ISO arena, the Message Handling System (MHS), which can handle many types of messages besides E-mail, provides an even better means of conserving bandwidth through a multicast-like method of distributed destination list expansion. The ISO MHS is discussed in further detail in section A-2.3.5.

### A-2.2.3 MPDT Teleconferencing

Teleconferencing is an application that allows multiple users to exchange text messages interactively, much like a telephone conference call. All parties receive (hear) all messages that are sent. At present, most teleconferencing systems (such as the World Wide Monitoring Command and Control System (WWMCCS)) operate by having all participating parties locally or remotely log onto the same host computer. As with mail systems, each destination receives a separate copy of the original message.

A centralized multi-endpoint connection, could be centered where the current conference host is, and outgoing traffic could be multicast to the parties involved in the conference. This would reduce outgoing traffic from the host by a factor proportional to the number of conference participants. It should be noted that the subsequent decrease in network traffic through the use of MPDT should also have a positive effect on delay, which has a greater impact on perceived performance in this application vs E-mail. Teleconferencing needs a reliable service to assure that message contents are not corrupted and to ensure message ordering.

### A-2.2.4 Packet Voice/Video Applications

Similar to teleconferencing, yet even more demanding, are packet voice and video applications. Multi-party voice/video conferences require delivery of large amounts of data to multiple destinations with strict delay requirements. While these applications can benefit from the increase in bandwidth efficiency that MPDT transmission mechanisms can provide, the impact of the overhead introduced by connection management and reliability on delays is still unknown. On the other hand, current voice systems can tolerate lost/garbled data to some extent, so enhanced reliability at a lesser cost in delay and other overhead may be preferable to guaranteed reliability.

### A-2.2.5 Distributed Databases / Processing

Distributed database and other distributed processing applications require a considerable amount of coordination to maintain synchronization of distributed operations. Through the use of MPDT, a multi-endpoint connection can be maintained between distributed application entities so that they all receive the same updates, control messages, etc. In addition to synchronization benefits, bandwidth can be conserved by multicasting updates to all recipients. As previously

mentioned, the ability to efficiently maintain distributed applications is also a plus to survivability concerns. Distributed databases generally require reliable service to ensure accurate updates, while other applications may be more tolerant of errors, and find an unreliable service acceptable.

### A-2.3 Current MPDT Research and Development Activities

In the following sections we describe a number of approaches to providing MPDT capabilities to networks. The items discussed range from proposed standards, to experimental implementations, and commercial products. They also range from application layer solutions to lower level network layer ones, and offer varying degrees of performance and reliability.

#### A-2.3.1 Proposed Draft Addendum to ISO 7498-1 on MPDT

The proposed draft addendum to the ISO's open systems interconnect (OSI) reference model (ISO 7498-1) was recently dropped by ISO as an active project. It expanded on the basic ideas of the existing model to facilitate inclusion of multi-peer data transmission at all seven layers (2). The addendum was not a protocol specification that describes how MPDT is to be carried out, but more of an architecture or framework providing the 'hooks' for adding multi-peer protocols to the ISO suite, just as the reference model defines the protocol layers, but no specific protocols. This was one of the primary reasons it was dropped.

The addendum called for significant additions to all seven layers of the reference model. In general, it extended all references to two entities cooperating in a transmission or connection to mean two or more entities. In addition, it defined group addresses and extended the definition of destination address fields to include lists of single and/or group addresses.

The addendum also introduced the notion of 'active group integrity' (AGI), and an associated integrity function to be applied to multi-peer connections. The integrity function was to be applied to multi-peer connections, and if certain conditions were not met, the connection would be dropped. An example of an active group integrity function might be that a connection between several hosts would be considered valid only if at least 80% of the group was participating/reachable, or perhaps a few critical hosts had to be present to constitute a valid connection.

Another significant feature of the addendum is that as the only ISO/OSI specific work on MPDT, it is the only one to address session and presentation layer network issues, though not much is said. As would be expected, the presentation layer would manage transfer syntax among members of the active group, while the session layer would maintain coordination and synchronization among presentation entities in a multi-peer session connection, utilizing an extended form of the token concept, passing it among all users of a connection.

Also of interest was that the addendum provided for multiplexing of more than one (N)-MPDT connection onto a single (N-1) connection, as well as splitting and/or spreading of (N)-MPDT connections onto more than one (N-1) connections. These provisions are needed to take maximum advantage of available bandwidth.

While ISO is no longer pursuing work in this area, the DoD's efforts to provide MPDT capabilities to its systems can benefit by studying the work that was performed. While the document may be flawed in some areas, others can be useful in providing the framework for a DoD specific MPDT implementation. The fact that it spanned all seven layers of the reference model brings out an important issue - that to fully utilize MPDT mechanisms, upper layers must have 'knowledge' of how to use them. For example, a network layer multicast service would be of little use to a transport layer that could only handle single destination transmissions.

### A-2.3.2 Internet Multicasting

Recently there has been much activity in the Internet community with respect to IP (network layer) multicasting. Internet Requests For Comments (RFCs) detailing host extensions for IP multicasting (RFC 1112) and a distance vector multicast routing protocol (RFC 1075) have been published and an experimental implementation is publicly available. IP multicasting provides an unreliable multicast service (as defined previously) at the network layer. Additionally, a paper has been presented outlining a reliable transport layer multicast protocol built on top of this work[6,7,8,9].

---

[6] S. Deering, "Host Extensions for IP Multicasting", RFC 1054, Stanford University, May 1988

[7] S. Deering, "Multicast Routing in Internetworks and Extended LANs", SIGCOMM Summer 1988 Proceedings, August 1988

[8] D. Waitzman, C. Partridge, S. Deering, "Distance Vector Multicast Routing Protocol", RFC 1075, BBN STC, Stanford University, November 1988

RFC 1112 utilizes IP class "D" addresses (i.e. the first four high order bits of the address are "1110") to denote a host group. In standard dotted notation, IP host group addresses range from 224.0.0.0 through 239.255.255.255. Two special addresses are also defined, the first host group address (224.0.0.0) is to be left unused, while the second (224.0.0.1) is defined as the permanent group of all IP hosts on the directly connected network. No provisions are made for addressing the set of all Internet hosts.

Given this addressing scheme, primitives are defined for hosts to join and leave groups for both the Internet and local network. Tables are maintained so that incoming multicast packets are delivered to the proper upper layer interface point(s). Transmission of multicast packets is essentially the same as for unicast packets except for the distinctive address class. On networks utilizing broadcast media such as IEEE 802.3, the packet will reach all local hosts automatically (provided their interfaces are programmed not to filter out multicast addresses), but for store and forward networks, and to cross network boundaries, IP multicast routers or some similar devices/mechanisms must be used to duplicate and forward packets to all hosts specified by the multicast address.

RFC 1112 also defines an internet group management protocol (IGMP) which is used by multicast hosts to report their group memberships to multicast routers. Rather than storing an explicit list of members for each multicast group address, multicast routers use IGMP to query hosts on their local network and keep a simple list of groups for which at least one host on the local network is a member. In order to reduce query traffic, all hosts listen to query replies, and suppress their replies for a given group when they hear another host respond. After some number of queries with no replies for a given group, it is assumed that no local hosts are interested in receiving multicasts for that group, so they are not locally transmitted by the router. When a host first joins a group, it forwards a reply message without waiting for a query, so the router's tables may be updated quickly.

The multicast transport protocol proposed by Crowcroft and Paliwoda[10] was designed with client/server applications in mind, but does not preclude peer-peer applications. This transport layer protocol adds

[9]J. Crowcroft, and K. Paliwoda, "A Multicast Transport Protocol", SIGCOMM Summer 1988 Proceedings, August 1988

[10]op. cit.

reliability to Deering's network layer multicast service. As with the multicast network layer protocol, an experimental implementation also exists. The protocol makes several assumptions that may not realistic. For example, it is assumed that the individual addresses of all members of a given group can be obtained. It is also assumed that multicast repeaters are available for networks that do not inherently have a broadcast/multicast capability. The paper also discusses an 'implosion' problem related to too many acks/replies arriving at the sender at the same time, and suggests randomized scheduling of replies as one solution. This area still requires more research to be performed before standardizing.

### A-2.3.3 Broadcast Service for X.25 Networks

Hughes Network Systems has published a description of their broadcast service for use in X.25 point-to-point networks utilizing their integrated packet network hardware (IPN 9000). The basic operation of the scheme involves the use of X.121 addresses for groups of destinations whic are static. The IPN 9000 provides both access to the broadcast service and acts as broadcast repeaters. The repeaters use standard X.25 connections to pass data between themselves, and to deliver data to local destinations. From the perspective of the source, broadcasts are point to multipoint, with return traffic via non-broadcast X.25 connections. The product includes network management functions to monitor and control the configuration of the broadcast network topology as well as monitors and logging of broadcast calls.

### A-2.3.4 Guaranteed, Reliable, Secure Broadcast Networks

A patent pending invention for providing a reliable and secure broadcast service has been described by Lawrence Tseung in a recent IEEE publication[11]. The idea behind the invention is to place additional hardware on a broadcast network to provide a 'replay' service to systems on the network that may have missed a previously broadcast message for any reason - even if the system was off.

The additional hardware consists of at least three components - a retransmission computer (RC), a designated recorder (DR), and one or more playback computers (PC). Systems wishing to reliably broadcast a message send it to retransmission computer via a reliable one-to-one transmission link. The RC then adds a sequence number and timestamp

[11] L. C. N. Tseung, "Guaranteed, Reliable, Secure, Broadcast Networks", IEEE Network Magazine, November 1989

information to the message, and broadcasts it to all systems on the network. While all systems on the network receive this broadcast, the designated recorder is the only one that sends an acknowledgement to the RC. If this acknowledgement is lost or the DR does not receive the message, the RC will retransmit. Once an acknowledgement is received, the RC proceeds to transmit the next message. In addition to sending acknowledgements, the DR also stores broadcast messages for a short period of time, in case any playback computers missed them. A PC can detect if it has missed anything by examining the sequence number of the message it has most recently received. If there is a gap in the number sequence, it recovers the lost messages from the DR over a one-to-one reliable link. In the event that many messages are being lost, a PC can request the DR to slow its acknowledgements to the RC. The PC(s) perform a similar message recovery function for the rest of the network, storing messages for a much longer period of time. Thus, whenever a system detects that it has missed a broadcast message, say after a local reboot, it can establish a one-to-one reliable link with a PC and receive copies of any missed messages (provided it has stored the timestamp/sequence number of the last message it received).

### A-2.3.5 OSI Message Handling System (MHS) (CCITT X.400)

The MHS has two key features that support multicasting of messages - multi-destination addressing and message duplication/splitting. Multi-destination addressing, as the name implies, permits the sender of a message to specify a list of addressees as its destination. In addition, this list of addresses may contain group addresses which stand for other such lists. Each group address is associated with a specific MTA within the greater MTS. All messages addressed to a given group are forwarded to this MTA for destination list (DL) expansion (group address translation). When a message first arrives at an MTA, its destination field is examined and group addresses associated with that MTA are replaced by the equivalent address list. This process is then repeated until all nested group addresses are also expanded. Checks are made to prevent endless list expansion in the case of recursive address references. Next, for singularly addressed (non-group) messages a routing function is performed to determine whether the message is to be delivered locally, or forwarded to another MTA for further handling. For multiply addressed messages, rather than making a copy of the message for each specified destination and routing them separately, the routing function is first applied to each destination address and then they are divided up according to their next 'hop' through the MTS. Copies of the

message are made for each set generated, and the destination fields of the copies are assigned the corresponding list of addresses before forwarding.

#### A-2.3.6 Tactical Communications

While a number of specialized systems have been developed for the tactical environment, most have the disadvantage of not interoperating with one another. For example, the Marine Tactical Systems Technical Interface Design Plan (MTS TIDP)[12] describes the ability to specify up to sixteen additional message recipients (addees) using routing indicators in the tactical header portion of a message. One bit is used for each separate destination. While this provides for a compact address list, it only works well for networks with a small number of users (sixteen) as the number of address bits required grows linearly with the number of users.

### *A-3 MPDT Issues*

In this section we revisit some of the protocols and mechanisms described above, and discuss the advantages and shortcomings to their various approaches to MPDT. In general we see that a reliable multicast is much more difficult than unreliable, and that more work is needed to determine the feasibility of some potential solutions.

#### A-3.1 Proposed Draft Addendum to ISO 7498-1 on MPDT

Of primary significance are the extensions to all seven layers of the OSI basic reference model in the areas of multi-destination addressing and multiplexing and splitting of data over connections. These extensions would allow for applications to have a standard method of access to multi-peer/multicast capabilities, with lower layers utilizing the most effective means for data delivery.

On the other hand, the PDAD was not without its shortcomings. The reassessment report noted that it is not clear whether or not connection oriented (CO) or connectionless (CL) transfers can be combined for a single group, and that while given a definition, it is not clear how decentralized MPDT actually works. In addition to lack of detail in some areas, there are other potential problems with the PDAD. Further, while the notion of active group integrity (AGI) seems like a nice feature on the surface, the potential overhead needed to track 50 or more members of a

[12]Technical Interface Design Plan For Marine Tactical Systems (MTS TIDP), Volume 5 - Protocol Standard

large teleconference or distributed database connection, with members dynamically joining and leaving, could be quite prohibitive. At present though, this area has yet to be explored, so it is not clear exactly how much extra network traffic and processing power would be needed to support such a feature. In fact, the PDAD did not even suggest methods which might be used to acquire the data necessary to determine AGI.

### A-3.2 Internet Multicasting

While the work to date with Internet multicasting is quite promising, it has a major drawback in that multicasts are not reliable. A reliable multicast service is needed, as it would be inefficient to require each application to provide its own reliability mechanisms on top of the multicast network service, when a single reliable service for use by any application could be made available.

Crowcroft and Paliwoda's proposed method of providing a reliable multicast capability on top of Deering's multicast service sounds promising, but is not without problems. First, it assumes some mechanism by which the total membership of a given group can be known by a transmitting host. Unfortunately, Deering's IGMP protocol is designed such that multicast routers need not know how many local hosts belong to a given group, so they are incapable of providing a list of specific hosts. One possible means of determining the set of all members would be to query the group and wait for replies. Alternatively, group membership lists could be maintained by directory services. But this does not solve the problem completely. Neither solution would respond well to rapid changes in group membership. More significant is the amount of overhead required by the protocol in transmitting hosts when a group's membership is large. As mentioned previously, an experimental implementation exists, so performance results should be available in the near future.

### A-3.3 Hughes Networks X.25 Broadcast Service

The major limitation of the Hughes scheme with respect to providing MPDT capabilities to DoD ISO protocols is that it relies on proprietary hardware and software. This aside,it also relies heavily on a human network manager to configure the connectivity between broadcast servers (repeaters), and can handle only 1000 group numbers (three digits). Furthermore, the assignment of these numbers must also be performed by the network operator. Once set up however, the system requires no further operator intervention though extensive monitoring capabilities are provided. For smaller networks (tactical systems) the reconfiguration

capabilities provided to the operator can be seen as a plus, while for large networks, reliance on a network operator to assign limited group numbers can only be a drawback.

### A-3.4 Guaranteed, Reliable, Secure Broadcast Networks

The primary advantage of Tseung's invention is that all hosts on a network are guaranteed to received messages broadcast using his scheme, even if they were not listening (or unable to listen) to the original transmission. Further, the sender need not slow its transmission pace to accommodate a few limited hosts on the network. It can transmit full speed to the retransmission computer, which will in turn transmit full speed to the rest of the network. Any slow systems unable to keep up can simply request copies from a playback computer.

On the down side, even though delivery is guaranteed, the sender does not know when a given system has received its message. In addition, all messages a transmitted at least twice - once by the originator, and again by the RC. On networks where the basic service is not subject to many errors, this may be unnecessarily wasteful. Further, while the delay for initial transmissions would be comparable to network layer service, the overhead involved in establishing one-to-one connections for message recovery make it quite expensive, especially when a large number of systems require retransmission. A final shortcoming is the reliance on a few specialized components. A faulty receiver on the designated recorder would completely disable the broadcast service, as the retransmission computer could never advance to its next message. Further, bandwidth would be wasted as the RC repeatedly attempted to retransmit its current message. Online backup systems could be provided at expense of added complexity and cost.

Care must also be taken in the placement of the designated recorder on some network topologies. If the DR and PCs are placed too close to the RC, during periods of heavy traffic load it is possible that the scheme could degenerate into many one-to-one requests for retransmissions, as the DR continued to acknowledge broadcasts that few other systems received correctly.

The applications that might benefit most from the type of service this scheme can provide appear to be distributed databases and transaction processing, as the forced sequencing of broadcast messages - a side effect of using the retransmission computer - simplifies the handling of updates and information requests. On the other hand, applications such as tactical systems that often operate over networks with high error rates

may find the scheme unsuitable, due to the high cost of retransmissions and unpredictable delay.

### A-3.5 OSI MHS (X.400)

As described above, the MHS provides an application layer multicast messaging service. The method of tying group addresses to specific MTAs is a trade-off between maximum efficiency and independence of MTAs. MTAs not supporting group list expansion will, by definition, not have any group addresses associated with them and thus not interfere with the operation of those that do.

### A-3.5 General Issues

Connectionless network layer multicasting appears to be an attractive mechanism for implementing an MPDT service, as it helps to overcome some significant problems presented by higher layer applications that must rely on lower layer unicast and/or (peer-peer) connection oriented network services.

Care must be taken in the implementation of a network layer service. Providing for lists of addresses in packet headers is not sufficient, and will not work in some cases. Network layer packets are typically quite small, and a list of even a few hundred destinations may exceed a maximum packet size that is practical for buffering limits in hosts. Thus group addresses should also be supported, and perhaps preferred.

If applications are to take full advantage of the broadcast/multicast capabilities inherent in many networks at the link and physical layers, simply having a multicast capability at the network layer is not sufficient. A standard method of accessing this service is needed, and if applications are to take advantage of the service, protocols at intermediate layers must be designed so that they do not interfere with or defeat the performance savings made available by network level multicasting. Furthermore, both reliable and unreliable services should be provided, so that applications can forego reliability when not essential, and not incur the additional overhead associated with reliable delivery.

Management of reliable multi-peer connections is another problem that needs to be addressed. With hundreds or even thousands of destinations for a single transmission, and data rates to those destinations that may range from megabits down to a few hundred bits per second, multi-peer transmissions may have to be slowed down to the least common throughput capacity of all group members. Crowcroft and

Paliwoda's window scheme does just this by setting the multicast transmit window size to "the lower bound of the smallest of the advertised receive windows". Alternatively, Tseung's scheme frees networks from being crippled by a few slow listeners by allowing them to miss the original broadcast and request a 'replay'. Of equal importance is the management of group membership. Hughes Networks method relies on a network operator making dynamic groups nearly impossible. Deering's method (IGMP) works well so long as a list of specific group members is not needed. While the ISO PDAD mentions AGI and the ability to join and leave groups at all but the physical layer, no further discussion is made as to how this might be brought about. More work is needed to determine exactly what group management functions are needed and how best to implement them.

### *A-4 MPDT Conclusions*

The previous sections discussed a wide variety of methods available for realizing MPDT capabilities, none of which appears to be an acceptable solution for all cases. What is needed then is an integrated set of protocols to provide an MPDT service that can meet these requirements while presenting a uniform interface to applications. Much work is still needed to realize this goal, though the groundwork has already been completed.

In the short term, the DoD should mandate support of the MHS's multicast capabilities and encourage the definition of group lists to provide bandwidth savings.

Not to be overlooked are the needs of tactical users whose traffic is atypical compared the rest of DoD (i.e. not mail/message oriented). For these users, the development of a network layer multicast protocol similar to what is available in the TCP/IP community, will provide a baseline unreliable datagram capability also in the short term. As many tactical applications involve constant or frequent updates of information (such as tracking and sensor data) reliable delivery is not essential to satisfy their needs. Other tactical uses of networking do require reliability, so work should also be pursued in this area for later implementation.

To realize long term goals, more research is needed in the areas of reliable multicasting, multi-endpoint connections, and group management. Fortunately at present, few applications require such capabilities, though some would certainly benefit.

# Appendix B: GOSIP Security

## *B-1. GOSIP Security Introduction*

Section 3.5 of this report reaches the conclusion that DoD must develop a Security Profile for its utilization of OSI security services and mechanisms. In support of that Security Profile development, this appendix provides background information on previous work and establishes possible solutions in the ISO framework. The appendix first presents a general approach to developing the security profile. It then defines security services in terms of the original DDN security architecture and finally discusses issues related to providing those services in an OSI environment.

## *B-2. Approach to GOSIP Security*

DoD needs to establish a profile which supports the security needs of individual DoD activities while promoting widespread interoperability. The profile must both define standard conventions for representing common security aspects and facilitate the requirement to connect heterogeneous systems.

The development of a DoD GOSIP security profile should interact with those ongoing activities considering security for large DoD applications. A particular instance is the ongoing security work for the Defense Message System (DMS). Previous experience, such as the DDN security architecture work of the early 1980's, has shown that development of a DoD wide security profile is a substantial undertaking which should be initiated as soon as possible with broad representation.

The DDN security architecture defined the placement of security services, specifically access control, authentication, authentication, availability (assured service), data confidentiality and data integrity, within the DoD internetworking architecture. This architecture recognized that different classes of users with varying security requirements needed to be served by the DDN. The architecture attempted to address this concern by devising security service elements that are capable of providing variable levels of protection.

The architecture defined security services at the application (access control and authentication), transport (integrity), network (access control, authentication, and data confidentiality), and link (confidentiality and traffic flow security) layers. The service layering provided in Section B-5 is based on the DDN security architecture.

As with the overall DoD GOSIP profile, the security portion of that profile will be an evolving document. The issues identified in section B-4 are areas to be addressed as part of such a profile. Certain issues can be addressed now, as part of an initial profile, while others require further study or must await the refinement of the related standard, as with IS-IS routing or network management information. The resolution of these other issues would be included in subsequent revisions of the profile. The approach is to present recommendations on these issues to a DoD wide forum, possibly as part of the PSTP, and incorporate the results into the DoD OSI profile.

### *B-3. Security Services for DoD*

There are a wide range of security services possible that need to be included in the GOSIP specifications. The security services that were considered necessary for DDN are: authentication, access control, confidentiality, data integrity, non-repudiation, audit, and assured service. Each of these are discussed in subsequent sections.

#### B-3.1. Authentication

Authentication establishes the validity of a claimed identity. In the context of data communications we consider source authentication, proof that the stated source sent the information, and peer authentication, proof that the communicating entities are actually those identified by the supplied addresses. Peer authentication is used during the establishment of an association between entities, i.e., call setup. Source authentication is used throughout during communications between entities to assure that all elements of the transmission are from the claimed sender.

#### B-3.2. Access Control

Access control protects resources accessible via the communications system from unauthorized use. The determination of authorization is made based on the authenticated identity of the communicating entity, and a set of rules governing access to the system. The greatest challenge in any access control system is determining the appropriate rules to use in granting or denying access. The access rules need not be identical across all systems. Some systems may grant one class of access (e.g., read and write access) while others may grant access on a limited basis, with some users may be allowed to write information into the end system and others are only allowed to read. The challenge for security engineers is assuring that the interconnection of systems with differing access rules does allow the violation of security policy.

### B-3.3. Data Integrity

A data integrity service protects information from malicious or accidental modification. There are three possible services which could be provided, first only correct information is passed on the service access point (SAP) (this implies that the protocols implementing this service provides reliability such as retransmission or forward error correction). Second information determined to be corrupt will be discarded and an indication of that event passed to the SAP. Third the information is passed regardless of it's integrity, but an indication is made of the validity of the information.

### B-3.4. Non-Repudiation

Non-repudiation is the service that protects the endpoints from the other denying that it received or sent a message. It either reliably notifies the sender when the recipient receives a communication or, provides the recipient with proof that the information received came from the sender, and that the sender will not be able to deny sending the information. This service is useful in military command and control, electronic contracting, and financial obligations.

### B-3.5. Audit

The detection of anomalous events must be recorded and reported, the audit service collects the information. The service may optionally also provide analysis and reaction services.

### B-3.6. Confidentiality

The confidentiality service provides that information is not made available or disclosed to unauthorized individuals, entities, or processes. This is the classic security service. There are two basic confidentiality services, data confidentiality, and traffic flow confidentiality. Data confidentiality assures that user data (N-user-data from a protocol standpoint) is protected from unauthorized disclosure. Traffic flow confidentiality assures that information concerning the presence or absence of information flows is protected from unauthorized disclosure.

### B-3.7. Assured Service

Assured service is a property of the communications system that attempts to prevent denial of service from occurring. Assured service includes assurances that the protocols in the system are free from

deadlock and livelock conditions, and that resource allocation and usage in the system is maintained on a "fair" basis.

Assured service is not provided solely by the security elements of a networked system, but by the overall network engineering and implementation of the network. Assured service is tightly coupled with the network management system.

### *B-4. GOSIP Security Issues for DoD*

A DoD Security Profile for OSI must provide a comprehensive specification allowing DoD organizations to acquire interoperable solutions to secure networking requirements. The profile should include the definition of specific mechanisms, their placement and integration in the protocol processing, the syntax and semantics of security information, and the management of security information and functions.

While the work discussed in section B-2 has driven towards defining how to go about addressing security requirements, the goal of the DoD OSI Security Profile is to define approaches in sufficient detail to allow independent agents to procure secure, interoperable systems.

#### B-4.1. End-System to End-System Security Protocol

The Secure Data Network System (SDNS) standards define SP3 and SP4, two very closely related end to end security protocol alternatives for providing the security services defined in Section 3 between end systems. Conceptually, SP3 and SP4 are versions of a security protocol which is located between the transport and network layers. SP3 is more closely associated with network layer processing (layer three) and SP4 is more closely associated with transport layer processing (layer four). SP3 and SP4 involve the use of SP with different, overlapping option subsets. The overlapping, interoperable subsets are part of the minimum essential requirements for each protocol. To support widespread interoperability, guidelines need to be established concerning how the attributes which dictate the selection of SP options are assigned and which capabilities are mandatory parts of implementations.

A number of factors need to be considered in selecting specific configurations guidelines. These factors include the constraints on network topologies, security properties and services offered, security implications for implementation options, and cost/performance impacts.

A major consideration in selecting a configuration is the support for diverse topologies. SP4 is an end system oriented option while SP3 is

intended to support encryption at both end systems and intermediate systems. Intermediate system solutions may be attractive in order to support specialized networks (such as some low bandwidth tactical applications), to realize cost savings (a single encryption device serving a collection of workstations), to accommodate evolvability and interoperability, and to support high performance LAN's (not imposing the encryption overhead within such a LAN, but only at gateways to and from it). Intermediate system encryption may also be used where the objective is to enforce access control at the boundary of an environment.

The security properties and services considerations primarily involve the granularity of cryptographic separation and the coupling of encryption with transport layer functions. The SP4 set of options supports distinct keys per transport connection and the coupling of transport sequence information with the encryption process when operating in the SP4-C mode. The SP4-E option has distinct keys per end system. The SP3 options are oriented only at distinct keys per end system. With the exception of the use of the SP4 final sequence number (FSN) option, key granularity is primarily a local implementation issue which must be consistent at both ends in order to realize the intended service.

An additional security issue is the allocation of functions to physical devices in a local implementation. There may be an advantage, in some instances, in providing security services in a front end. The SP3 and SP4-E options simplify the required host to front end interface where security functions are provided externally for an end system.

### B-4.2. Peer Entity Authentication

Authentication is an issue in a number of areas in the OSI environment. One specific instance, addressed below, is the subject of authentication of network control information. The issue addressed here is one of how DoD will specifically provide the authentication services needed throughout OSI, and particularly those services which are user oriented. One of the essential distinctions in defining authentication schemes is a determination of whether the authentication is performed between two points, or whether information is being authenticated from one source to multiple destinations (either through multicast service or as a result of posting as in a directory). For pairwise authentication, encryption can establish peer entity authentication when coupled with appropriate key management (for example end system authentication as part of the SP3 or SP4 service). For multipoint authentication, or when a third party validates information, a public key based approach is appropriate. X.509 (DIS 9594-8) and the ISO draft authentication framework describe the

use of public key based certificates to provide strong authentication where needed. For X.509, this is tightly coupled with the need to perform authentication in support of directory activities. Public key based authentication for DoD use would involve different algorithms and formats than those in X.509 and must be defined.

Several OSI standards now have placeholders for authentication and access control information. All of these standards leave the definition of the authentication and access control information and of the use of that information as open issues. At the application level, this authentication sometimes takes the form of transformations performed on data objects prior to transfer between end systems. The DoD profile must address the algorithms (see 4.8) and usage conventions for providing authentication and the identification of attributes to be authenticated by DoD in those instances where authentication is required. A question that has arisen is whether DoD's operational framework results in any differences in the way in which organizational and role issues are handled in the case of directory service oriented authentication.

### B-4.3. Security Policy and Services

The DoD OSI security profile should have at least an informal statement of the security policy(s) which the profile is implementing. The policy should include the security rules and properties which are to be preserved in a network implemented according to the profile. These rules cover access control, integrity, authentication, and assured service.

Access control includes confidentiality and involves describing the granularity of objects to be distinguished and the nature of the rules to be enforced. The manner in which heterogeneous environments are supported must be included in the policy statement.

Integrity properties in this context include only message transfer integrity. Coupled with authentication, this involves establishing the guarantees to be provided that information communicated between applications is delivered unaltered and that the identity of the source of that information can be relied upon.

The description of the assured service properties and services is more difficult to describe. The intent is to express the reliance that can be placed on the network to meet quality of service requests in various situations. The content of a policy and service description and the degree of formalism to be employed is an area both for further research

(into expressing assured service and integrity properties) and for further consideration.

### B-4.4. Access Control

Access control involves protection against unauthorized use of resources accessible through OSI protocols. This service may be performed as part of the network, transport, or application layers. Access control is concerned with both the protection of user or end system assets from remote entities and the protection of communication resources from unauthorized users. Frameworks for conveying access control attributes and performing access checks has been defined as part of the SDNS program and within the ISO. Further, many OSI standards include placeholders for access control information to be exchanged between peer entities. The nature of the information to be exchanged, however, is not addressed.

The access control portion of the DoD OSI profile must address two primary areas. The first area is establishing DoD guidelines on the nature and format of commonly expressed and interpreted access control attributes. The second area is access control approaches for those applications, including management and directory functions, which have not been fully covered under SDNS.

The access control schemes need to be closely coupled with authentication approaches. Access control decisions can be based in part on the attributes authenticated through public key certificates. These attributes will need to correspond between the authentication and access control approaches. A part of this determination includes a decision concerning which attributes will be part of access control decisions performed at the application layer (primarily user, process, and object information) and which attributes will be part of decisions at the network/transport layers (primarily end system identity and possibly session if associated with a specific application).

### B-4.5. Intermediate Systems

There is a large issue concerning security for intermediate systems, i.e. routers, gateways. This area largely breaks down into protection of the routing function, protection of network control transactions, and special security related functions. Based on the scope of this profile, i.e. definition of DoD OSI-based protocols, the emphasis is on requirements for the routing oriented protocols, end system to intermediate (ES-IS) and

intermediate system to intermediate system (IS-IS), and on the network management protocols, covered in Section 4.10.

The routing protocols (ES-IS and IS-IS) need to be authenticated and need to be supplemented to support security concerns. These concerns include supporting security as an attribute in route calculation and in protecting against threats from malicious (or malfunctioning) routers (acting singly or cooperatively).

For the ES-IS protocol, the primary security concern is authentication. This is particularly important for the exchange of configuration information associated with announcing the presence of an ES or IS to other network entities. The authentication mechanism should provide multi-destination authentication. Beyond the authentication function, the only supplemental feature is the inclusion of security attributes in the quality of service field contained in redirect PDU's. This inclusion supports the indication of security related redirection information.

Security aspects of the internet routing function which require supplements to an IS-IS protocol are part of an area for further study. Those aspects must be an integral part of the evolving concept for routing. Issues to be considered as part of security based routing include what security attributes are a part of the route determination process (e.g. security levels, protection services, administrative domains), how those attributes are communicated and authenticated, and how to factor those attributes into the overall route calculation algorithm. Another issue is how to handle the problem of containing flawed or malicious routing information from legitimate IS's. This problem involves providing a capability for validating, or selecting, dynamic information propagated from other IS's.

### B-4.6. Interoperability and Evolution

While this is not actually a profile issue, it is an essential area for making OSI based security work within DoD. Multiple protocol stacks as well as existing security equipment will require the interconnection of heterogeneous security systems. Further, US DoD systems will need to interoperate with other systems representing other US Government organizations or other non-US systems. How these interconnections will be handled securely is an important part of the overall plan and should at least be recognized, if not resolved, as part of the OSI profile.

The first issue to be addressed in this regard is interoperability between SDNS based OSI solutions and BLACKER systems. A number of

approaches are possible including secure gateways, superencryption (SDNS over BLACKER), and BLACKER modifications. Key management is a major issue to be addressed in this area.

### B-4.7. Connectionless vs. Connection Oriented Service

This is a particular instance of interoperability which is receiving initial consideration in GOSIP VERSION 2. If both connectionless and connection-oriented environments (TP-4 over CLNS and TP-2 over CONS) are to be concurrently supported, then the interoperability between the two needs to be addressed. While this is a general OSI problem, it is particularly acute from a security perspective and from a DoD perspective. The situation arises regularly with regard to operation in Europe and within NATO. Since solutions tend to involve termination of lower layer protocols (transport and below), either security approaches which rely upon the end to end nature of those layers must be modified or the solution to the problem must be changed. Alternative solutions involve application relays (with their attendant security problems) and the selection of common end to end protocols. This is particularly a problem for DoD operation where there is significant security reliance on transport layer services provided in TP-4.

### B-4.8. Algorithms

One of the major areas of divergence between DoD systems and other applications of the OSI security services will be in the selection of cryptographic algorithms to be used for confidentiality, integrity, and authentication services. While algorithm flexibility exists within OSI, these conventions need to be defined for DoD use. DoD should define algorithm identifiers within the OSI algorithm context. A classified annex can then be generated covering applicability guidelines and descriptions of algorithms for use in DoD systems and an identification of the associated parameters. While incorporation of these identifiers into the OSI registry might be desirable, this may be impractical. Such registration would require submission of the identifiers and related characteristics through ANSI to ISO.

A related important issue is the design of interfaces to cryptographic algorithms which allow for changes to the algorithms (such as for replacement or evolution) without the need to redesign the surrounding system. Such a generalized interface is an important step in the DoD use of commercial protocol implementations, substituting military grade algorithms for commercial algorithms.

### B-4.9. Application Functions

Many of the security concerns specific to mail are addressed by combinations of the SDNS Mail Security Protocol (MSP) and by aspects of the 1988 version of MHS (X.400). DMS activities will consider additional requirements needed to meet DoD formal message system needs. While not a complete treatment, these activities form a strong base for addressing mail specific security requirements. No such corresponding attention has been given to security for FTAM, VT, and other applications (including those built upon the Remote Operations and Association Control services). Application security is the subject of research within both DoD and ISO. The National Computer Security Center is currently addressing the security issues at the application layer.

### B-4.10. Network Management Security

The OSI Management Framework is receiving considerable attention as a focus for the management of heterogeneous networks. This framework defines management service primitives and a management protocol (CMIS and CMIP). These basic capabilities then operate on Management Information Bases (MIB's) which provide the collection of managed information and objects. A great deal of attention has gone into defining appropriate MIB's, both in the OSI context and for TCP/IP systems.

#### B-4.10.1. Protection of Management Functions and Data

From a security perspective, concerns primarily involve protecting the management protocol exchanges and in protecting the contents of the MIB. The protection of management protocol exchanges are essentially specific applications of general security services discussed elsewhere. For the management exchanges (and for other exchanges of network control information which may take place between network entities), this involves providing data origin authentication, peer entity authentication, and connection integrity with recovery. Many of these concerns, along with confidentiality where needed, will be provided by the underlying communication service. The additional requirement to be addressed for DoD is the authentication and access control information provided within the CMIP exchange. (The same access control and authentication information might equally well be incorporated within an SNMP exchange.) The nature of such authentication, where applied, needs to be defined.

The second area is the protection of individual elements of the MIB. This is largely a subset of the general database security problem. The notion

of different classes of access (read, write, update) exists and needs to be expanded to associate different protection classes. This is consistent with the concept for the MIB. An approach for meeting selected MIB security requirements without requiring trusted network entities throughout the internet can be based on providing intrinsic protection for individual security critical MIB entries. This approach might indicate the need for strong authentication on selected entries (a digital signature on software items), finer granularity confidentiality of selected items (through access control lists or encrypted entries), and accountable actions (selective auditing on a per entry basis). The profile in this area will define standard protection classes and mechanisms for providing them where needed in DoD systems.

The profile should also provide guidelines on those classes of MIB entry which require special protection. This portion of the profile relates to the general concern about the security of distributed algorithms and functions. The susceptibility of such algorithms, and the managed objects associated with them, is an area that must be addressed on a case by case basis. Software maintenance, time synchronization, remote configuration, topology, routing, and protocol parameters are all areas to be considered.

### B-4.10.2. Management of Security

The management of security information and mechanisms in networks is sometimes called out as a distinct requirement area. Security management areas include key management; security audit collection and processing; and management of access control, identification, and authentication information. With the stronger protection afforded the management services described in B-4.10.1, these capabilities should be realizable within the overall management framework. The one possible exception requiring further study is support for security audit functions.

The profile in this area should identify security related MIB entries. This has already taken place for some key management related items. Special handling required for the local processing of these items may also be discussed. The area of network security audit information also needs to be further addressed.

Key management services have been addressed in reasonable detail as a part of SDNS. The largest open area to be addressed within key management as part of a security profile is how to handle multi-destination associations, particularly as may be needed to support multi-point data transmission (MPDT) approaches.

### B-4.11. Security review of DoD OSI profile

The previous areas have concentrated on security specific mechanisms and approaches in OSI. This emphasis reflects the desire to adopt, where possible, the results of the open standards efforts. The OSI standards have also driven towards providing general frameworks in which individual profiles can be constructed, such as for DoD. The issue areas are those aspects of the framework where individual systems must make specific selections in order to insure interoperability and to determine a degree of security protection appropriate for their environment.

Review of the complete protocol profile's mechanisms and approaches is needed to insure that the resulting profile provides a comprehensive set of services needed to meet DoD's operational requirements. A part of this review includes consideration of the security implications of choices made for options within individual layers. Part of the security of a DoD OSI profile relies upon choices made within individual protocols such as the selection of checksum type and use, sequence number size and application, and security labels. These choices need to be reviewed in the context of security to insure an overall consistent treatment for DoD.

The transport protocol profile is a particularly important example from a security perspective. To provide security at the transport layer, security mechanisms such as packet sequence numbering, checksums, packet reordering, and retransmission are required. In addition to mandating TP-4 in most instances, this will require constraining the TP options and negotiation rule.

## *B-5 GOSIP Security Conclusions*

The DoD Security Profile must insure that all of the services defined in section B-3 are adequately addressed. However, as section B-4 discussed the final solutions are not readily available at the present time. So like the original GOSIP the Security Profile will have to be an evolving document. As issues are resolved the Security Profile should be updated to reflect each resolution. Ultimately, there will be a Security Profile which supports secure yet interoperable network communications.

## Appendix C: DoD Message Handling System (MHS)

### *C-1. DoD Message Handling System (MHS) Overview*

The Department of Defense (DoD) and other U.S. Government Agencies are moving toward a standardized set of communication protocols described in the Government Open Systems Interconnect Profile (GOSIP). Version 1.0 of GOSIP recommends the 1984 International Standards Organization (ISO) specification for a Mail Handling System (MHS). The MHS specification was updated in 1988 to give it more flexibility and capability (and still be compatible with 1984 MHS). The more recent (1988) MHS specification has been identified as being more easily modified to meet DoD concerns. For this reason, the 1988 MHS specification has been selected as the basis for the DoD electronic mail system. (The Multicommand Required Operational Capability (MROC) document for the Defense Message System (DMS)[1] provides additional MHS requirements.) It should be noted that most vendors implement the 1984 MHS specification, acquisition authorities should specify a "technology upgrade" clause if products are needed now that can be upgraded to the 1988 specification later. This appendix outlines three areas of improvement to meet DoD communication needs:

Priority levels
Security
MHS Multicasting capability

These are bases of potential additions to the 1988 X.400 specification and are discussed in the following paragraphs.

### *C-2 Priority*

The existing MHS specification permits three priority levels to be used by end users (urgent, normal, non-urgent), these are designed to fit into the priority recommendations made earlier in the report. Other Military Messaging systems such as AUTODIN provide more than these three levels. This mismatch can be accommodated by using a NATO MHS component, the User Agent (UA) which has however many priority levels defined for use by end users and providing mapping of these levels to the three level available in the lower level components of the MHS as follows:

UA priority level 8 - MTA Urgent
UA priority level 7 - MTA Urgent

[1]Multicommand Required Operational Capability (MROC), Defense Message System (DMS) memorandum dated 6 February 1989.

UA priority level 6 - MTA Normal
UA priority level 5 - MTA Normal
UA priority level 4 - MTA Normal
UA priority level 3 - MTA Normal
UA priority level 2 - MTA Non-Urgent
UA priority level 1 - MTA Non-Urgent

Although only three transport priority levels are available, eight levels are preserved at the UA level. Therefore, eight levels of priority can be provided even in the frequent case that the transport service cannot provide any distinct services to different priority levels. The advantage to this approach is that off-the-shelf lower level MHS components and Mail Transfer Agents (MTA) could be used by the DoD.

*C-3 Security*

The security section of the report recommended the SDNS Key Management Protocol (KMP) and Security Protocol (SP-3I) to provide a basic level of security for all end systems requiring security. An additional granularity of security to the message level can be provided using the Message Security Protocol (MSP). This protocol resides between the MHS User Agent (UA) and the Message Transport Service (MTS). The MSP protocol makes efficient use of the encryption process and key management by encryption all of the duplicate messages using a single message key. The message key is then encrypted in a unique manner for each of the individual messages using publicly posted keys2. However, the use of these security components need to be determined in a Security Profile.

*C-4 MHS Multicasting Capability:*

An optional multicasting capability exists within the 1988 MHS specification that permits limited multicasting capability. Section 14, Procedures for Distributed Operation of the MTS specifies an efficient implementation of smart splitting/duplication of multiple delivery messages. It is noted that in section 14.1.1 a loop-hole existed as follows: "Neither the procedures shown nor the order of processing steps in them necessarily imply specific characteristics of an actual MTA". To obtain more efficient use of network bandwidth and possible time savings when sending duplicate messages, the DoD MHS should implement this

[2]SDNS Secure Data Network System Message Security Protocol Specification SDN.701, Revision 1.2, dated November 3, 1988.

option. As more efficient lower layer services can be offered, they should be utilized by DoD MHS.

## Appendix D: FTAM Recommendations

### *D-1.1 FTAM Overview*

Of the many military issues under consideration, most deal with services and features found in protocols which reside below the File Transfer, Access and Management (FTAM) protocol[1,2,3,4]. This is particularly true of Multi-Homed End Systems, Quality of Service, and Network Management issues. For the most part, these issues have no effect on FTAM. A strict interpretation of the issue of Multi-Peer Data Transmission calls for a service which is simply inappropriate for FTAM to provide. This interpretation requires a single copy of a file to be injected into a network and transmitted simultaneously to multiple file service users. FTAM is end-system intensive and is not designed for this type of operation. The only major deficiency found in FTAM has to do with its ability to meet the security needs of the military.

FTAM must support network management services. FTAM services (Kernel, Read, Write, File Access, Limited File Management, Grouping, Recovery and Restart) are required by CMIP as specified by the OSI/NM Forum to support movement of large amounts of data for network management applications. (Note: this is not to be confused with the NIST OSI Implementors' Agreement standard.) These all exist within FTAM at this time. Future FTAM implementations must further support network management as manageable objects with defined MIB elements.

### *D-1.2 FTAM Security Improvements*

Security is the one area where FTAM will need substantial enhancement if it is to meet military needs. While some security features such as passwords have been included in FTAM, they only offer protection against inadvertent access and casual attacks. It would be relatively easy to exploit FTAM through an active attack.

---

[1]ISO, Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management Part 1: General Introduction, ISO/DIS 8571/1, August 7, 1986.

[2]ISO, Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management Part 2: Virtual Filestore Definition, ISO/DIS 8571/2, August 7, 1986.

[3]ISO, Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management Part 3: The File Service Definition, ISO/DIS 8571/3, August 7, 1986.

[4]ISO, Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management Part 4: The File Protocol Specification, ISO/DIS 8571/4, August 7, 1986.

In FTAM, passwords are used for a variety of access control purposes. Passwords can be required for access to the filestore, to establish the application association regime, and for access to the file itself in the file selection regime. Individual passwords may be required to allow the file access actions read, insert, replace, erase, extend, read attributes, change attributes, delete, create, and re-create (delete and create anew). There are, however, two major deficiencies with the FTAM password feature. First, the ISO specification does not require the encryption of passwords by FTAM. Moreover, GOSIP 2.0 explicitly states that FTAM is not responsible for password encryption. The second deficiency is that FTAM does not discuss how the password is to be authenticated.

The security of the real filestore itself is an area which is not mentioned at all in FTAM. GOSIP 2.0 states that the responsibility for the security of the real filestore rests with each local system. So FTAM itself plays no role in filestore security other than to convey access passwords. Total security in a network sense therefore cannot be assured since there could be a large diversity of implementations with differing levels of protection.

Other security deficiencies in FTAM include the lack of data sensitivity labels on the File Access Data Units as they are packaged for transmission over the network[5]. There is also no protection against playback and spoofing. To prevent these attacks, FTAM should include some type of handshaking mechanisms and liveliness assurance procedures such as timestamps or synchronized clocks. As FTAM stands today, for example, it would be fairly simple for an attacker to deny service by injecting an F-ABORT or F-TERMINATE primitive into the FPDU stream.

More subtle problems exist in FTAM with respect to assurances that it actually receives the services from the lower layers that it requests. There are no assurances that information is passed up from the lower layers uncorrupted. Since FTAM does not employ a checksum for error protection, it cannot be assured that the information in a FPDU has not been altered.

[5]M. D. Abrams,, Ed., "Trusted Network Interpretations of Criteria from DoD 5200.28-STD," The National Computer Security Center, February 7, 1987.

### *D-1.3 FTAM Recommendations*

We recommend that effort be expended to provide FTAM security features. Specification of the detailed changes required to rectify the security deficiencies in FTAM are estimated to be substantial.